ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 41, No. 4: 725-736, December 2013
http://dx.doi.org/10.7469/JKSQM.2013.41.4.725

시스템엔지니어링을 적용한 ISEP 개발에 관한 연구

변보석 *† · 최요철 * · 박영택 *

* 성균관대학교 기술경영학과

Development of the ISEP Based on Systems Engineering

BoSuk. Byun *† · YoChul. Choi * · Young T. Park *

* Department of Management of Technology, Sungkyunkwan University

Abstract

Purpose: The purpose of this study is to propose an Integrated Safety Evaluation Process (ISEP) that can enhances the safety aspect of the safety-critical system. This process utilizes the advantages of the iterative Systems Engineering process combined with the safety assessment process that is commonly and well defined in many standards and/or guidelines for railway, aerospace, and other safety-critical systems.

Methods: The proposed process model is based on the predefined system lifecycle, in each phase of which the appropriate safety assessment activities and the safety data are identified. The interfaces between Systems Engineering process and the safety assessment process are identified before the two processes are integrated. For the integration, the elements at lower level of Systems Engineering process are combined with the relevant elements of safety assessment process. This combined process model is represented as Enhanced Functional Flow Block Diagram (EFFBD) by using CORE® that is commercial modelling tool.

Results: The proposed model is applied to the lifecycle and management process of the United States aircraft system. The US aircraft systems engineering process are composed of twelve key elements, among which the requirements management, functional analysis, and Synthesis processes are considered for examplenary application of the proposed process. To synchronize the Systems Engineering process and the safety assessment process, the Systems Engineering milestones are utilized, where the US aircraft system has thirteen milestones. Taking into account of the nine steps in the maturity level, the integrated process models are proposed in some phases of lifecycle. The flows of processes are simulated using CORE®, confirming the flows are timelined without any conflict between the Systems Engineering process and the safety assessment process.

Conclusion: ISEP allows the timeline analysis for identifying activity and data flows. Also, the use of CORE® is shown to be effective in the management and change of process data, which helps for the ISEP to apply for the development of safety critical system. In this study, only the first few phases of lifecyle are considered, however, the implementation through operation phases can be revised by combining the elements of safety

• Received 22 October 2013, accepted 7 December 2013
† Corresponding Author(bsbyun@lsis.biz)

activities regarding those phases.

Key Words: Systems Engineering Process, Safety Assessment Process, Integrated Safety Evaluation Process

1. 서 론

과거의 많은 시스템들은 원하는 기능들을 구현하는 것에 많은 노력을 기울였다면, 현대의 시스템들은 주변 환경, 외부 시스템, 사람 등에 미치는 영향들을 더욱 중요하게 고려하는 추세이다. 그 중에서도 녹색 성장 시대에 맞춰서 사람들은 시스템(예: 철도)의 안전을 최우선으로 생각하고 있으며, 안전성 확보와 관련한 기술은 이미 사회적으로 꼭 필요한 기술로 인식되고 있다[5, 6].

시스템 안전성 확보 문제는 대형 공공 시스템, 군방 시스템, 민수 시스템 등 다양한 분야에서 제기되고 있으며, 최근에는 교통 시스템과 관련하여 많은 여론이 집중되고 있다. 교통 시스템은 한 나라의 경제력에 영향을 미치는 물류 시스템의 근간이며, 일반 사람들이 주변에서 손쉽게 접하고 영향을 받는 범용적인 대형 복합 시스템이기 때문이다. 이는 교통 시스템의 안전 문제는 개인뿐 아니라 나라에 까지 큰 영향을 끼칠 수 있음을 의미한다.

시스템 안전을 확보하기 위해서는 다양한 방법들이 존재하지만, 기본적으로는 시스템 초기에 시스템의 위험원(Hazard)을 식별하는 것이 가장 중요하다[Clifton 2005, 1-94]. 다시 말하자면, 시스템을 개념 단계에서부터 시스템의 위험원을 파악하고 시스템이 개발 주기 동안 진화됨에 따라 시스템의 위험이 제거되고 경감되도록 시스템을 개발해야 한다. 즉, 시스템 개념 단계부터 시스템의 개발까지 잘 정의된 프로세스에 의해 시스템이 개발되어야 하며, 이는 시스템엔지니어링 프로세스를 기반으로 안전성 평가 프로세스가 이루어져야함을 나타낸다.

시스템엔지니어링 프로세스를 기반으로 안전성 평가 프로세스가 이루어지기 위해서는 이 두 프로세스 사이의 인터페이스를 명확히 해야 한다. Papadopoulos 등(1999)의 연구를 기반으로 많은 분야에서 이 둘의 조화를 중요시 생각하고 이를 적용하려고 하고 있지만, 둘 사이의 명확한 인터페이스를 제시하는 논문 및 자료가 대형 복합시스템의 시스템 수준이 아닌 컴포넌트 수준(H/W, S/W)의 인터페이스 연구만이 활성화 되고 있는 수준이다[Papadopoulos and McDermid 1999, 47-66].

본 논문에서는 미 항공 시스템의 사례를 기반으로 시스템엔지니어링 프로세스와 안전성 평가 프로세스의 인터페이스를 명확히 하고, 이 두 프로세스를 통합한 프로세스 모델을 제시하고자 한다. 이를 통하여, 각각의 프로세스가 어떠한 활동과 데이터가 흐르는지를 나타냄과 동시에 두 프로세스의 데이터 흐름을 나타냄으로써, 둘 사이의 인터페이스를 분명하게 하고자 한다.

제안하는 프로세스 모델은 기본적으로 시스템 생명주기를 고려하였으며, 이와 동시에 반복적인 시스템엔지니어링 프로세스를 기반으로 설계되었다. 시스템 생명주기는 시스템의 개념 단계에서부터 실제 운용 및 폐기 단계까지 모든 단계를 포함하며, 특히 개념 및 설계 단계를 집중적으로 고려하였다. 그리고 시스템의 각 수준에 대해 시스템엔지니어링 프로세스를 반복적으로 수행하면서 시스템을 점진적으로 개발하는 반복적인 시스템엔지니어링 프로세스를 통해, 시스템의 점진적인 진화 양상을 나타내었다.

본 논문은 서론에 이어 제 2장에서는 ISEP 모델의 개념, 제 3장에서는 ISEP 모델의 개발 방법, 그리고 제 4장에서는 미항공 시스템 사례 기반의 ISEP 모델링 결과에 대해 기술한다. 마지막으로 제 5장에서는 본 연구의 결론 및 토의를 통해 논문을 마무리 짓는다.

2. ISEP의 개념

본 논문에서 말하는 ISEP(Integrated Safety Evaluation Process)란, 시스템엔지니어링 프로세스와 안전성 평가 프로세스를 점진적인 개발을 고려하여 시스템 생명주기에 맞춰서 하나의 모델로 통합한 평가 프로세스 모델이다[Byun 2013]. 하나로 통합했단 의미는 시스템엔지니어링 프로세스에 맞춰서 시스템이 개발될 때 안전성 평가 프로세스는 이와 동시에 어떻게 수행되며 두 프로세스 사이에 어떤 데이터가 오가는지를 명시한 것을 말한다.

시스템엔지니어링에서는 일반적으로 요구사항 분석, 기능 분석, 조합 등을 핵심 프로세스로 나타낸다. 여기서 안전성 평가 프로세스는 전문 공학(Specialty Engineering)으로 분류되며, 시스템엔지니어링 프로세스에 맞춰서 안전성 평가가 이루어진다[Cecilia 2006, 13-16]. 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 생명주기의 각 개발 단계에 따라 두 프로세스가 어떠한 활동을 하고 어떤 데이터를 주고받는지에 대해 명확하게 기술된 자료가 없다. 각각을 설명하는 자료는 있지만 시스템엔지니어링 프로세스에서 어떠한 데이터가 안전성 평가 프로세스에서 쓰이는 지를 명확하게 규정한 자료가 없다. 또한 프로세스의 설명이 문자로 기술되어 있기 때문에 이를 이해하는데 어려움이 있다. ISEP는 이러한 문제점을 해결하기 위해, 전산 도구를 기반으로 하나의 그래픽 모델에 두 가지 프로세스를 나타내고 둘 사이의 인터페이스를 직관적으로 나타내기 위함이다.

ISEP은 CORE®라는 시스템엔지니어링 전산도구를 사용하였으며, 도구 안의 EFFBD(Enhanced Functional Block Diagram)를 통해 모델링하였다. 그래픽 모델 활용으로 각각의 프로세스의 이해를 증진시켰으며, 전산 도구의 도움으로 프로세스의 내용을 효율적으로 접근 및 관리할 수 있다. 또한 제안하는 프로세스가 원하는 흐름대로 활동과 데이터가 흘러가는지 시계열(Timeline) 분석을 통한 시뮬레이션이 가능하다. 이로 인해 프로세스 적용을 위한 프로세스 조정(tailoring) 활동이 용이하며, 조정된 프로세스에 대해 적용 전 비용 및 기간을 분석할 수 있는 토대가 될 수 있다.

3. ISEP 모델의 개발 방법

ISEP의 모델을 구성하기 위해 우선적으로 모델링할 프로세스가 수행되는 시스템의 생명주기를 분석하여 각 시스템 개발 단계를 정의하였다. 이후, 시스템엔지니어링 프로세스와 안전성 평가 프로세스의 활동 및 데이터를 식별하고 이를 시간 흐름에 따라 프로세스 각각을 모델링 하였다. 마지막으로 모델링된 각각의 프로세스를 서로 주고받는 데이터를 식별함으로써 서로의 인터페이스를 식별하여 통합하였다. 이 때, 시스템의 각 생명주기 별로 먼저 크게 모델링하고, 이후 각 시스템 레벨 별로 반복적으로 수행되는 시스템엔지니어링 프로세스를 기준으로 반복적인 시스템 개발 양상을 모델링하였다. 이를 그림으로 표현하면 아래 <Figure. 1>과 같다.

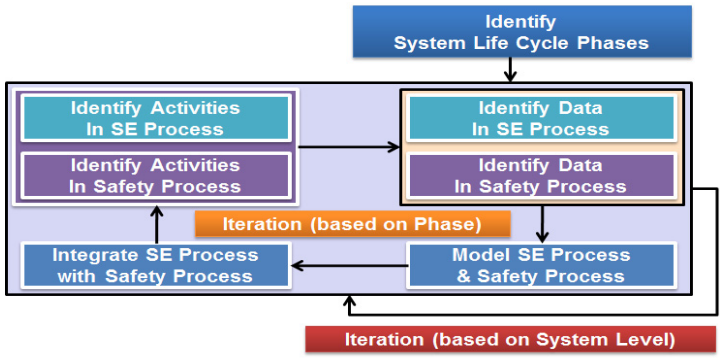

Figure 1. The Procedure for Modeling the ISEP Model

ISEP 모델의 구성은 우선 <Figure 2>와 같이 크게 3 수준으로 나눌 수 있다. 제일 상위 수준은 프로세스를 시스템 생명주기 관점에서 바라보는 것이다. 시스템의 생명주기는 시스템의 개선 등으로 인해 순환될 수 있으므로, 최상위는 생명주기 순환을 고려하여 표현하였다. 두 번째 수준은 각 시스템 생명주기 단계 별로 수행되는 시스템엔지니어링 프로세스와 안전성 평가 프로세스를 나타내었다. 세 번째 수준은 시스템엔지니어링 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 EFFBD를 통해 모델링되었다. 모델링을 위한 전산 도구로 CORE®를 사용하여 도구 내의 DB로 모델에 대한 데이터를 보관하였다.

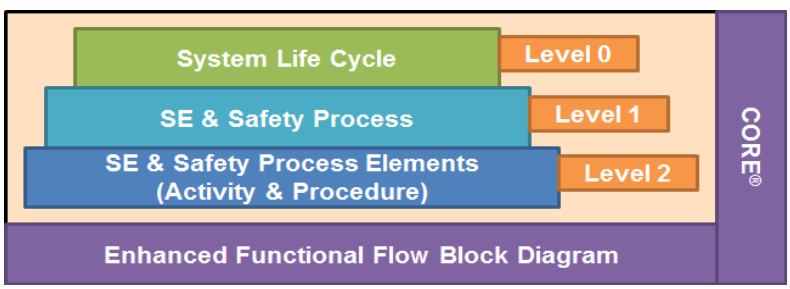

Figure 2. Hierarchy of the ISEP Model

EFFBD는 기본적으로 기능과 기능의 흐름을 나타내는 선, 그리고 기능 흐름을 나누는 OR, AND, LOOP, ITERATION 게이트로 작성된다. 그리고 기능에서 흐르는 데이터들을 일반 데이터와 trigger 데이터로 분류하여 표현한다. 제안하는 모델에서는 각 프로세스 활동을 기능으로, 프로세스/활동 흐름은 기능 흐름으로, 프로세스에서 쓰이는 입출력 데이터들은 일반 데이터와 trigger 데이터로 표현하였다. 각 프로세스들의 입출력 데이터를 표현할 때 데이터 모델링의 복잡성을 일관되고 단순화하기 위해 하위 6가지의 기준을 가지고 모델링을 수행하였다.

- 프로세스들의 feedback은 표현에서 제외한다.
- 특정 데이터를 획득하는 활동들은 모델에서 제외한다.
- 프로세스의 활동이 생명주기의 2단계 이상에 걸쳐서 수행되는 경우에는 각 단계에서 수행 하는 다른 활동으로 구분하여 표현한다.
- 데이터를 주는 활동과 받는 활동이 같은 OR 게이트 안에 포함되지 않고 받는 활동이 독립 적인 OR 게

이트에 속해있으면 일반 데이터로 표현 한다.

- 특정 활동에 반드시 필요한 데이터들은 모두 trigger로 표현한다.
- 하위 활동에서 쓰이는 일반/trigger 데이터들은 상위 활동에서도 같이 표현한다.

하위 활동에서 쓰이는 입출력 데이터들을 상위 활동에서 표현할 때, 3가지를 고려해서 일반 데이터로 표현할 것인지 trigger 데이터로 표현할 것인지 선택해야 한다. 첫째로, 출력 데이터를 발생시키는 하위의 활동이 해당 활동 흐름의 어디에 존재하는가. 두 번째로, 하위 활동에서 출력되는 데이터의 종류가 어떤 것인가. 세 번째로, 데이터를 입력받는 하위 활동이 해당 활동 흐름의 어디에 존재하는가. 해당 기준을 고려하여 결정되는 상위의 데이터 종류는 <Table 1>과 같다.

Table 1. The criteria for selecting trigger or normal data

Low-level Send Activity	Low-level Output Data Type	Low-level Receive Activity	High-level Data Type
Anywhere	Normal	Anywhere	Normal
Last Activity	trigger	Nothing	trigger
Last Activity	trigger	First Activity	trigger
Last Activity	trigger	Middle/Last Activity	Normal
First/Middle Activity	trigger	Anywhere	Normal

4. 미항공 시스템 사례 기반의 ISEP 모델링 결과

4.1 미항공 시스템의 생명주기

미항공 시스템의 생명주기는 Fig. 3과 같이 다섯 단계로 구성되며, 각 단계는 다시 세부 단계로 나누어진다. 다섯 단계는 임무 분석, 투자 분석, 해결책 구현, 서비스 제공, 그리고 폐기이다[FAA-a 2006]. 본 논문에서는 세부 단계를 모델에 반영은 하였지만 명시적으로 나타내지는 않았다.

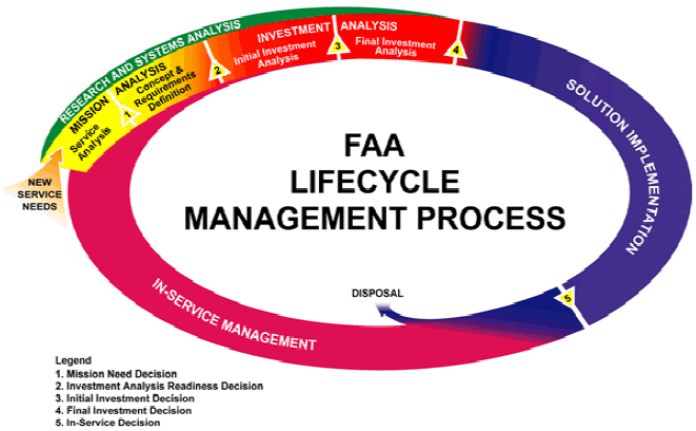

Figure 3. USA Aircraft System Life Cycle (FAA 참조, 2006)

Fig. 3과 같은 생명주기를 Fig. 4와 같이 모델링 하였다. 다섯 단계를 하나의 기능으로 표현하고 하나의 단계에서 다음 단계로 넘어가는데 이용되는 데이터를 표현하였다.

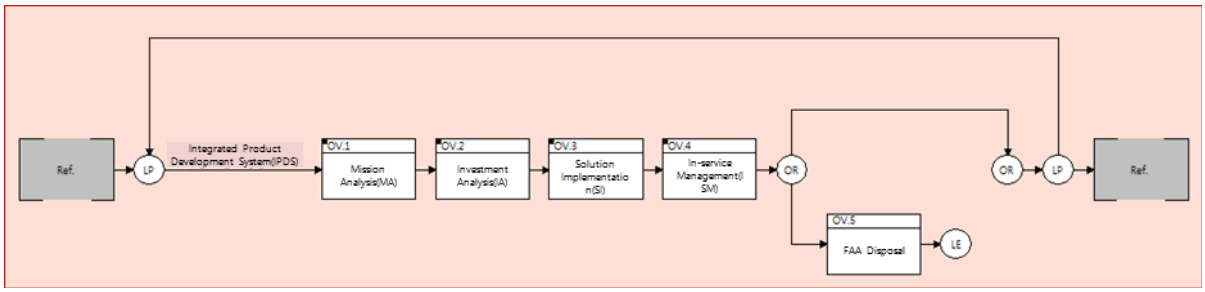

Figure 4. Integrated Process Model (Level 0: System Life Cycle View)

4.2 미항공 시스템의 시스템엔지니어링 프로세스 및 안전성 평가 프로세스

미항공 시스템의 시스템엔지니어링 프로세스는 Fig. 5와 같이 총 12개의 구성요소가 존재한다[6]. 이 중 본 논문에서는 시스템엔지니어링 핵심 프로세스로 분류되어 있는 요구사항 관리(Requirememts Management), 기능 분석(Functional Analysis), 합성(Synthesis) 프로세스만을 고려하였다.

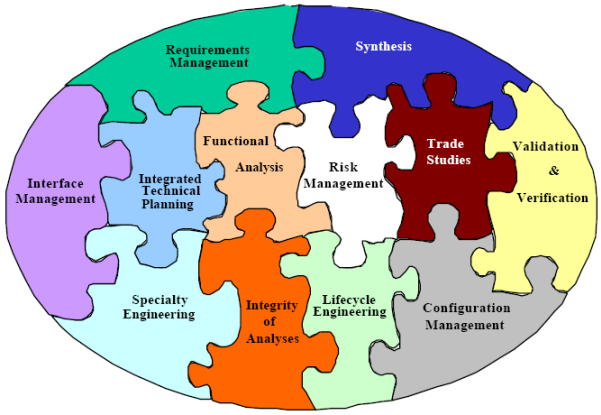

Figure 5. USA Aircraft Systems Engineering Element

안전성 평가 프로세스의 경우는 시스템 생명주기에 따라 Table 2와 같이 존재한다[7].

Table 2. Safety Assessment Process in each Phase of System Life Cycle

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	Hazard Tracking and Risk Resolution, Sub-System Hazard Analysis, System Hazard Analysis Operational & Support Hazard Analysis, Health Hazard Analysis, System Hazard Assessment Report, System Safety Program Plan, Safety Action Record
In-Service Management	Provide Status Reports

시스템엔지니어링 프로세스와 안전성 평가 프로세스의 수행을 동기화하기 위해, 시스템엔지니어링 마일스톤(Milestone)을 활용하였다. 시스템엔지니어링 마일스톤은 프로세스를 진행하면서, 검토가 필요한 중요한 시점을 나타낸다. 미항공 시스템에서는 대표적으로 13개의 마일스톤이 존재한다[8].

- CDR - Critical Design Review
- FBR - Functional Baseline Review
- FCA - Formal Configuration Audit
- IARR - Investment Analysis Readiness
- 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

프로세스를 표현함에 있어 시스템엔지니어링 프로세스의 반복 수행을 나타내기 위해, 미항공 시스템의 성숙 단계에 대한 9 단계를 고려하였다: 개념 형성, 개념 적합성 평가, 개념 개발, 저-사실성 모델링, 고-사실성 모델링, 표본 시스템, 제풍 성숙, 제품 승인, 그리고 서비스 제공[9].

시스템엔지니어링 프로세스, 안전성 평가 프로세스, 시스템엔지니어링 마일스톤, 그리고 시스템 성숙 단계를 고려하여 Fig. 6과 같은 모델을 개발하였다.

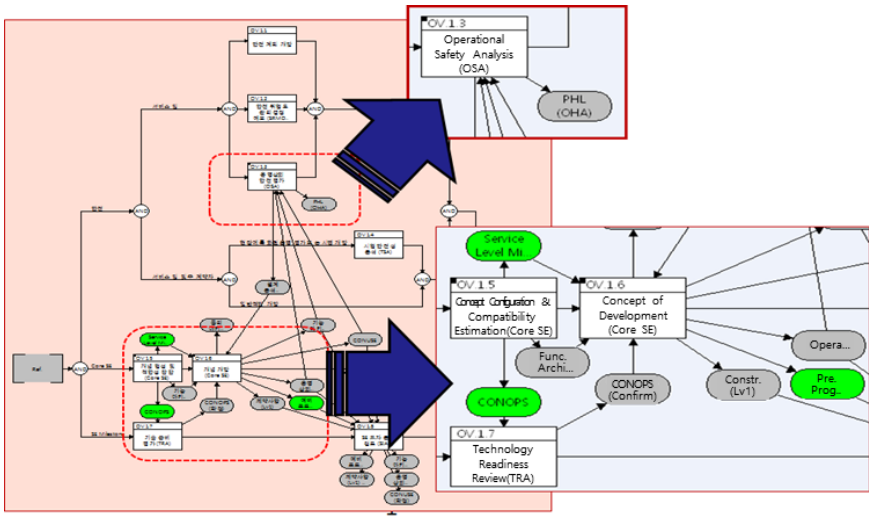

Figure 6. Integrated Process Model in Mission Analysis Phase (Level 1: Process View)

각 성숙 단계들은 시스템엔지니어링마일스톤으로 수행 시기가 분류 가능하므로, 모델에서도 성숙 단계의 끝에 해당 마일스톤의 내용이 수행되도록 trigger 데이터를 이용하여 연관성을 표현하였다.

4.3 ISEP의 세부 활동 흐름

반복적인 시스템엔지니어링 프로세스에 대한 안전성 평가 프로세스를 나타낸 모델의 하위에는 시스템엔지니어링 프로세스의 구성요소들의 절차와 안전성 평가 프로세스의 세부 활동들에 대해 표현하였다. 이 수준에서 시스템엔지니어링의 구성요소들이 각 반복 단계마다 어떠한 입출력 데이터가 있는지 나타나며, 안전성 평가의 경우에도 실제 분석 기법들에 대한 데이터들이 식별된다. 시스템엔지니어링프로세스 내용은 Fig. 7, 안전성 평가 프로세스의 내용

은 Fig. 8과 같다.

각 생명주기 및 성숙 단계마다 모델을 구축하였으며, 특히 임무 분석 단계와 투자 분석 단계가 상세히 표현되었다. 이는 시스템엔지니어링 핵심 프로세스가 주로 임무 분석 단계와 투자 분석 단계에 많은 비중을 차지하기 때문이다. 또한 해결책 구현 단계에서는 설계를 위한 아키텍처를 관리하고 실제

설계 전문가들의 비중이 커지며, 후반부에는 검증 및 확인 프로세스가 많은 비중을 차지하게 된다. 이러한 이유로 통합 안전성 평가 프로세스에서 다루는 범위가 벗어나므로 모델 또한 앞의 두 단계에 비해 나머지 생명주기 단계들은 상세함이 떨어진다.

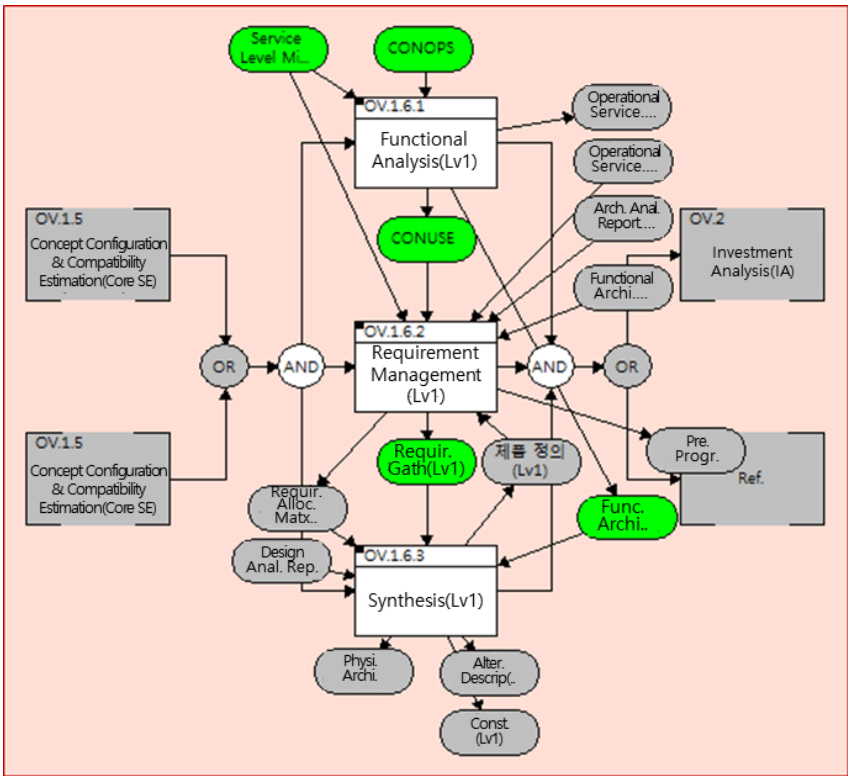

Figure 7. Concept Formulation & Feasibility in Mission Analysis Phase (Level 2: SE Process Element View)

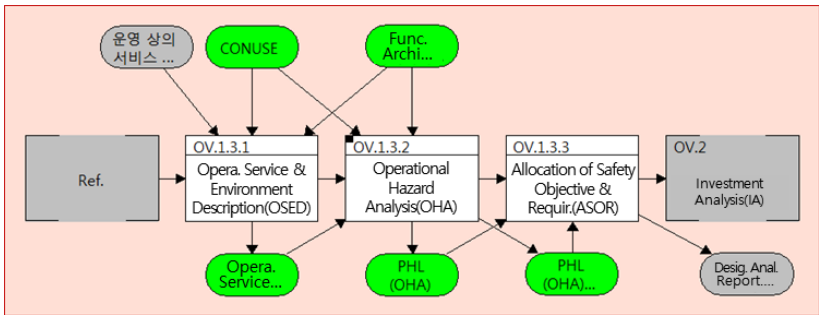

Figure 8. Operational Safety Assessment in Mission Analysis Phase (Level 2: Safety Process Element View)

4.4 ISEP 시뮬레이션

시스템엔지니어링 핵심 프로세스에 맞춰 안전성 평가 프로세스의 생명주기에 ISEP를 구축한 모델은 Fig.9 와 같다.

구축한 모델이 실제 흐름의 상충 없이 잘 수행되는지 파악하고, 각 프로세스의 수행 시기가 서로 원하는 시기에 수행이 되는지 시뮬레이션을 통해 확인하였다. 확인을 통해 trigger 데이터에 의한 프로세스 수행 시기 등의 오류를 확인하고 수정하였으며, 실제 미항공 시스템 사례와 비교하여 잘못된 부분들을 확인하고 최적화 된 통합 안전성 평가 프로세스 모델을 구현하였다. 최종적으로 시뮬레이션 결과 전체 흐름이 바르게 수행되고 있음을 Fig. 10을 통해 확인하였다.

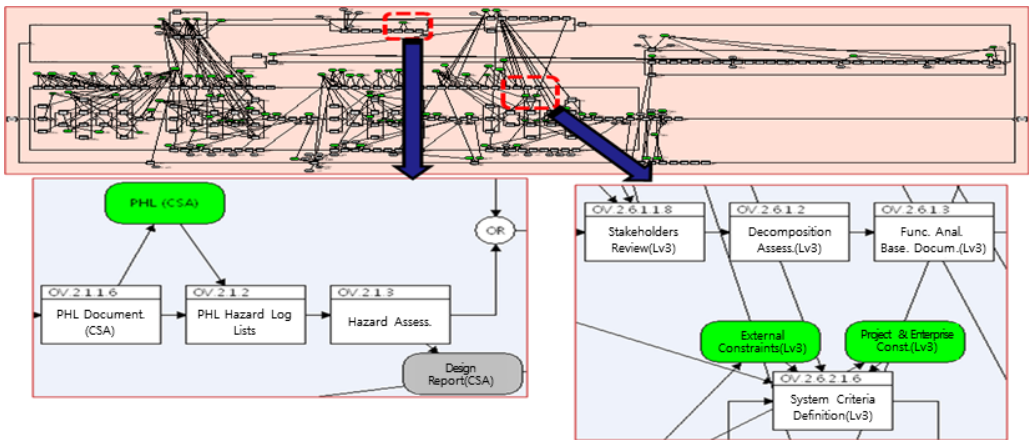

Figure 9. ISEP Model(Systems Engineering & Safety Assesment Process)

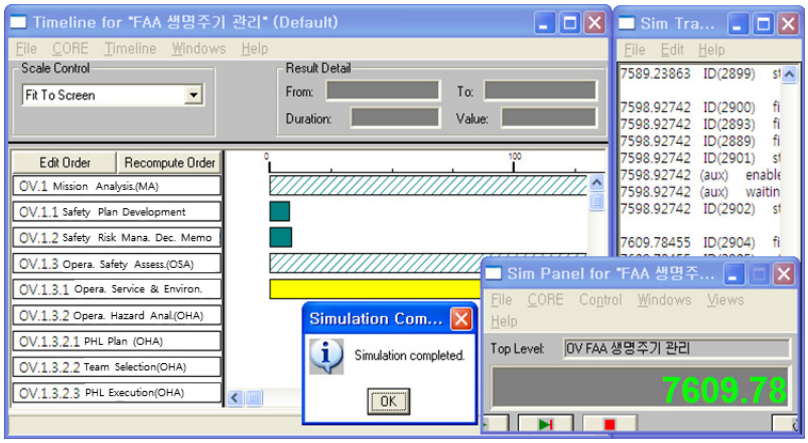

Figure 10. The Verification about the Integrated Process Model using Simulation

5. 결론 및 토의

미항공 시스템 사례를 기반으로 시스템엔지니어링 프로세스와 안전성 평가 프로세스의 인터페이스를 파악하고 두 프로세스를 통합하는 프로세스 모델을 제시하였다. 이에 따라 두 프로세스 간의 입출력 데이터를 확인하고 서로의 수행 시기를 확인하였으며, 시뮬레이션을 통해 프로세스 모델이 의도한 바대로 구축되었는지 확인하였다.

제시한 모델을 통해, 안전 중시 시스템 개발에서 시스템의 안전성 평가를 어떻게 시스템의 생명주기 상에서 수행할지 참고할 수 있다. 또한 프로세스를 조정하여 적용할 때 조정된 프로세스를 쉽게 검증하고 개선할 수 있다.

현재까지는 시스템 생명주기 상의 앞 단계에 집중되어 모델이 구축되었지만, 향후에는 실제 시스템 구현 및 운영 단계에서의 안전성 평가의 내용을 보충할 필요가 있다. 또한 모델에서 표현된 시스템엔지니어링 핵심 프로세스만으로는 안전성 평가 프로세스와의 연계가 부족하므로, 모델에서 제외된 검증 및 확인 프로세스나 형상관리 및 품질관리 프로세스 등을 통해 모델이 보완되어야 할 것이다.

REFERENCES

Byun, B. S. 2013. “Development of the Acquirer-focused Railway ISEP and RAMS Template Based on Systems Engineering.” Ph.D Dissertation, University of Sungkyunkwan(Submitted).

Cecilia Haskins. 2006. Systems Engineering Handbook. INCOSE 9:13-16.

Clifton A. Ericson II. 2005. Hazard Analysis Techniques for System Safety. John Wiley & Sons, INC. 1-94.

Ju, Yong Jun, and Lee, Yong Chul. 2011. “The Importance-Performance Analysis(IPA) of Service Quality According to Buying Experience of Rail Tours.” Journal of the Korean Society for Quality Management 39(1): 34-44.

Kim, Heun Jung, and Kim, Su Wook. 2013. “An Empirical Study of Railroad Technology Improvement Using AHP and QFD.” Journal of the Korean Society for Quality Management 41(2):301-321.

Papadopoulos, Y., and McDermid, J. A. 1999. “The Potential for a Generic Approach to Certification of Safety Critical Systems in the Transportation Sector.” Reliability engineering & system safety Journal 63(1):47-66.

The Federal Aviation Administration(FAA-a). 2006. System Engineering Manual Version 3.1. FAA. 1-3.

The Federal Aviation Administration(FAA-b). 2006. System Engineering Manual Version 3.1. FAA. 1-2.

The Federal Aviation Administration(FAA-c). 2006. System Engineering Manual Version 3.1. FAA. 4. 2-22.

The Federal Aviation Administration(FAA-d). 2006. Safety Risk Management Guidance For System Acquisitions Version 1.4. FAA. 34.

The Federal Aviation Administration(FAA-e). 2006. System Engineering Manual Version 3.1. FAA. 4. 2-31.