모델기반 시스템공학 기법을 통한 시스템설계 및 안전프로세스 통합모델의 구현에 관한 연구
On a Model-Based Systems Engineering Approach to the Realization of the Integrated Systems Design and Safety Process Model

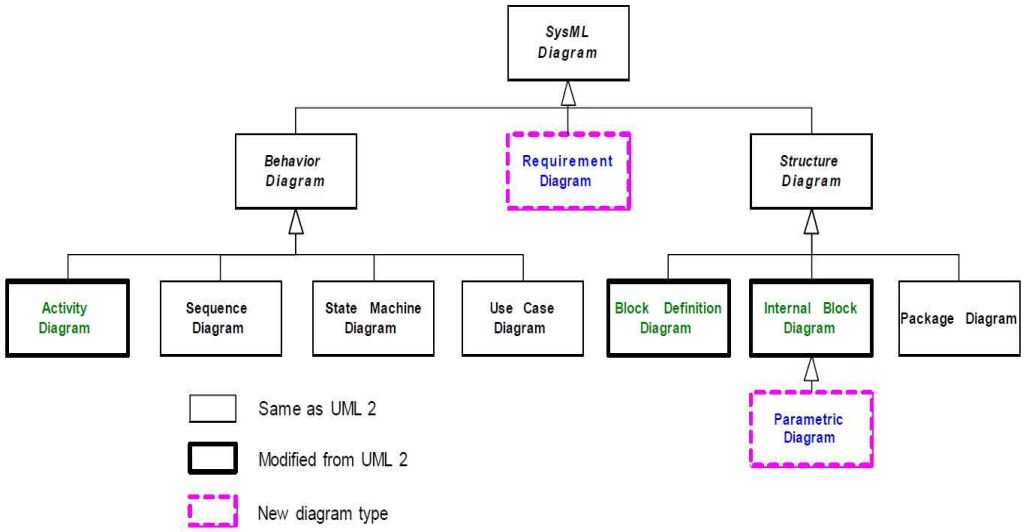
김 영 민* · 이 재 천*
Young-Min Kim* · Jae-Chon Lee*

Abstract

산업기술의 비약적인 발전으로 인해 오늘날 우리가 개발하거나 사용하는 시스템은 보다 기술의 고도화 양상을 보이고 있다. 따라서, 기존의 시스템이 지니고 있어 제공하는 단일 특성에서 벗어나 다양한 학제간 결합된 기술로 기존 시스템이 지니고 있는 관념적인 기능에서 벗어나 다기능을 제공하고 있다. 이로 인해, 기존의 개발단계에서는 보다 높은 설계 신뢰성이 요구되고 있다. 특히, 오늘날 우리사회는 시스템의 개발 성공이라는 안도에서 벗어나 시스템 운용·유지단계에서도 안전성 측면에서 매우 중요성을 인식하고 대비하고 있다. 따라서, 국내에서는 미흡한 상위 단계에서의 설계활동과 또한, 같은 시스템 수명주기 상에서의 시스템 안전활동을 동시에 고려한 동시공학적인 접근에 관한 연구를 본 연구팀은 지속적으로 수행해왔다. 따라서, 기존의 연구결과인 설계와 안전을 동시에 고려한 통합 설계 프로세스 모델에 대해, 시스템개발에 관련한 모든 이해당사자가 공통된 이해를 바탕으로 시스템설계와 안전 활동에 대해 상호 호완성과 공통된 인식을 갖고 접근할 수 있는 방안을 본 연구를 통해 수행하였다. 따라서, 본 연구는 모델기반 시스템공학 기법중 보편적인 언어인 공통 언어를 통해 기존 연구를 통해 제시한 통합설계 프로세스 모델을 구현에 관한 연구 수행을 통한 접근 방안에 관하여 논의하고 있다. 본 연구를 기반으로 향후 추가 연구를 수행한다면, 국내 대형복합시스템의 설계단계에서의 안전성을 동시 고려한 시스템 설계 신뢰성 확보를 위해 도움이 될 것으로 기대 된다.

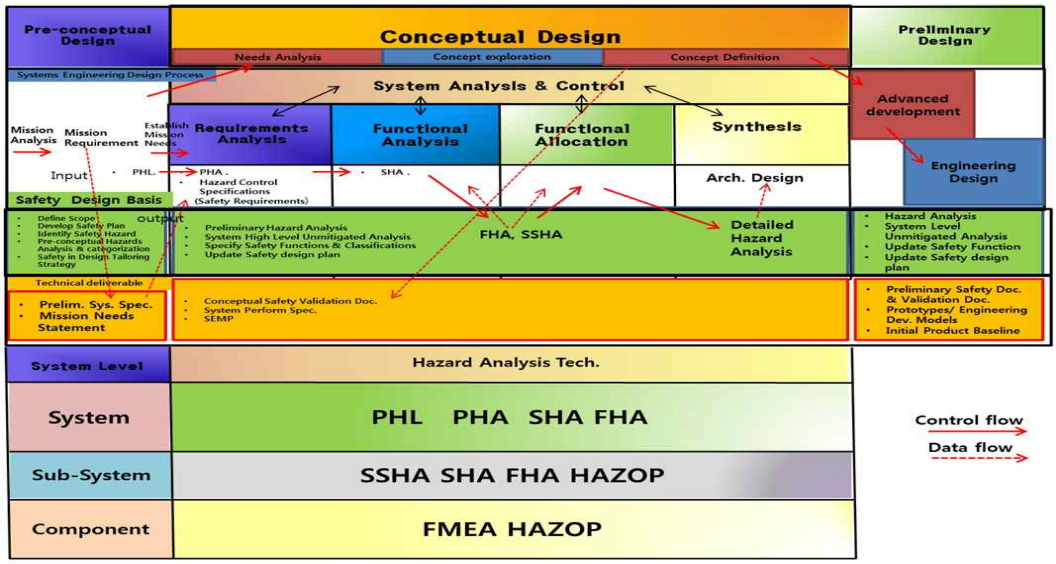
* 아주대학교 시스템공학과

1. 서 론



<Figure 1> Types and classes of SysML diagrams.

최근 들어 원자력·고속철도 등 우리가 사회를 살아가면서 생활하는데 있어서 중요한 기반시설로서 대형복합 안전중시 시스템이 우리생활에 중요한 역할을 하며 자리 잡고 있다. 이러한, 안전 중시 시스템이란, 시스템으로부터 발생하는 사고가 발생시 인명·재산 등 수많은 피해를 유발시키는 시스템을 안전 중시 시스템이라고 한다[1}. 이렇듯, 오늘날 과학기술의 진보와 인간의 편의성의 욕구를 충족시키기 위해 개발된 대형복합 안전중시 시스템은 최근 해외에서 발생한 일본의 후쿠시마 원자력 사고, 중국의 고속열차 탈선사고 등 인간으로 하여금 큰 재앙을 유발하여 국제적 불안감을 초래하였다. 이에 따라, 국내에서도 원자력 발전소, 고속철도, 무기체계 등의 대형복합 안전중시 시스템으로부터 국민의 안전을 보호하기 위해, 많은 노력을 기울이고 있다. 하지만, 이러한 시스템 안전확보를 위한 안전 대응에 있어서, 기존의 설계단계에서 초점에서 벗어나 운용 및 유지보수 단계에도 보다 많은 노력을 기울인다는 점은 환영할 일이다. 하지만, 이러한 활동에 있어서 이종간 학문의 상호유기적인 활동이 이뤄지지 못하고 개별적인 활동에서 머무르고 있다. 또한, 국내 뿐만 아니라, 해외에서도 설계단계에서의 시스템 안전성을 추구하는 활동이 상세설계단계에서의 기능안전성 중심에서 벗어나지 못하는 제한적인 활동에 초점을 두고 이뤄지고 있는 현실이다[2].



<Figure 2> The integrated process model quoted from the previous study

따라서, 본 연구진은 다년간 시스템 개발의 초기단계에 해당되는 개념설계 단계에서의 설계활동과 안전활동과의 상호 유기적인 영향에 관한 연구를 수행하여 시스템 설계 활동과 시스템안전 활동과의 상호운용에 관한 연구 수행을 통해, 통합된 형태의 설계 프로세스 모델을 구축하였다. 기존 연구의 취지는 시스템 초기 설계활동인 상위레벨에서의 설계활동과 시스템 안전 활동과의 상호 운용성을 동시에 고려하여 수행함으로써 시스템 설계 엔지니어와 안전 활동을 수행하는 엔지니어 사이의 상호운용에 관한 연관성에 대해 연구를 수행하였다. 이로서 시스템 개발에 있어서의 관련한 이해당사자간의 일관된 이해를 바탕으로 성공적인 시스템 개발을 수행하고 시스템설계의 상위단계에서 안전활동 및 위험원 식별에 따른 제거를 수행하기 위해 설계단계에 반영함으로써, 초기 설계 및 안전활동에 집중함으로써 보다 시스템 개발에 성공적으로 접근하리라 생각한다. 따라서, 본 연구진은 기존의 연구수행 결과를 시스템 개발에 관련한 모든 이해당사자로 하여금 공통된 이해를 바탕으로 개별 전문분야(Domain)에서도 이해할 수 있도록 모델 기반 시스템공학(Model-based systems engineering, MBSE) 기법을 적용시켰다.

특히, 이러한 문제 해결을 위한 방안으로 본 연구에서는 SysML[3](System Moleling Language)을 통해 해결하고자 한다. SysML은 적용시킨 이유는 기존 시스템 개발에 있어서 국제 표준으로 사용되었던 UML(Unified Modeling Language)의 확장된 새로운 개념의 표준이다. 이러한 SysML의 특징과 장점을 살펴보면, 우선 가장 큰 장점은 표준언어라는 점이다. 따라서, 이해당사자간의 정보를 공유하는데 있어서 동일한 이해를 가능하게 할 수 있다. 또한, 기존에 설계 및 안전활동을 수행하므로 발생된 결과의 문서가 문서중심의 산출물이라는 점에서 그래픽화된 모델링 언어로써 보다 목

표에 대한 정보를 효과적으로 전달 가능해진다. 앞에서 언급했듯이 시스템 개발 전산 지원도구에서 SysML지원을 확장하는 추세이다. 따라서, 오늘날과 같이 대형복합 안전중시 시스템에 대해 설계하고 안전활동을 수행함에 따라 무수히 많은 산출물을 발생시킨다. 이러한 결점을 보완하기 위해, 시스템 모델링 언어를 지원하는 툴을 활용함으로써 보다 체계적으로 개발에 다가 갈수 있을 것이다. <Figure 1>에서 제시되는 것처럼, SysML은 크게 3가지 특성인 거동, 요구사항, 구조적 특징 가진다. 따라서, 본 연구팀의 선행 연구를 통해 개발된 통합설계 프로세스 모델을 모델기반 시스템공학 기법중 하나인 SysML을 통해 구현함으로써 누구나 공통된 이해를 갖게 하고자 본 연구를 통해 접근적 해법을 제시하고자 노력하였다.

2. 본 론

2.1 모델기반 시스템공학 기법을 통한 통합 설계 프로세스 구현의 범위 및 목표

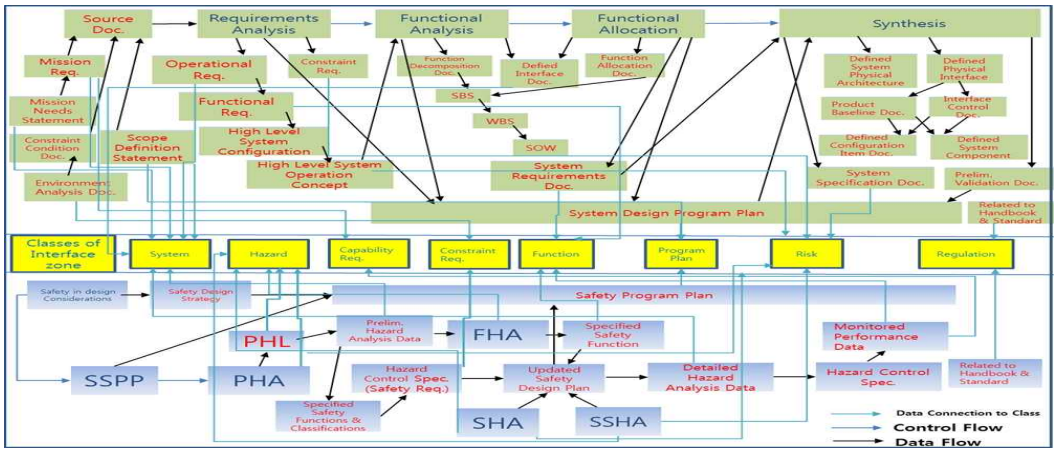
모델기반 시스템공학 기법 중 하나인 SysML을 활용하여 기존 연구수행을 통해, <Figure 2>를 통해 제시한 통합 설계 프로세스 모델 구현에 관한 연구수행은 시스템의 전 수명주기 상에 개념설계 단계에 해당한다. 따라서, 이번 연구를 통해, SysML을 통해 구현하고자하는 연구범위 또한 개념설계 단계에 초점이 맞춰있다. 따라서, 본 연구를 통해 <Figure 2>와 <Figure 3>의 기존 산출물인 시스템공학 설계활동과 시스템 안전 활동의 통합된 형태의 프로세스에 대해 SysML을 통한 구현 방안에 대한 제시를 하고자 본 연구를 수행하였다.

2.2 MBSE 기법을 통한 통합프로세스 모델의 구현을 위한 SysML 특성 분석

서두에 언급했듯이, <Figure 1>을 통해서, SysML이 크게 3가지(거동,구조,요구사항) 특징을 가지고 있고 이러한 측면에서 반영할 수 있다는 것을 알 수 있다. 본 연구단계는 통합설계 프로세스를 SysML 특성을 이해하여 반영하기위해, SysML 개별 다이어그램이 지니고 있는 특성을 분석하였다. 분석결과는 아래 <표 1>과 같이 정리하였다.

<Table 1> The results of SysML Diagrams Analysis

Diagram 종류	특징	관련내용
Activity Diagram	1.활동들의 흐름을 표현한다. 2.상태(State) 다이어그램 내부의 진행중인 과정의 확장형태.	시스템의 구성 및 기능 정의
State Diagram	1.상태(State), 전이(Transition), 사건(Event), 활동(Activity)로 구성된다.	상태의 변화 정의
Use case Diagram	1.시스템과 시스템과의 상호연동이 있는 액터 사이의 관계를 표현 2.시스템 행동을 조직화하고 모델링하는데 중요	기능 흐름 정의
Block Definition Diagram	1.시스템과 해당 시스템을 구성하는 요소를 표현하는 단위로서 Block과 Block간 관계를 정의	시스템 구성요소 정의
Internal Block Diagram	1.Block 내부구조를 표현한다. 2.어떠한 Block의 구성요소간의 관계를 표현하거나 구성요소간 접속관계를 표현한다.	시스템 내부 구성요소 정의
Sequence Diagram	1.모델 요소간의 상호작용을 시간적으로 표현하는 것. 2. 모델 요소의 협조에 의해 실현되는 거동을 표현하기 위한 다이어그램.	시간적 흐름 정의
Interaction Diagram	1.상호작용 다이어그램은 시퀀스 다이어그램과 커뮤니케이션 다이어그램으로 구성 2.객체와 객체 사이의 관계와 메시지로 구성	상호작용 정의
Package Diagram	1.Block 모델 요소군을 그룹화하기 모델 2.Package 간의 관계를 표현하기 위한 다이어그램	그룹화 정의
Class Diagram	1.각 클래스, 인터페이스, 협동 사이의 관계를 나타냄. 2.객체들을 추상화한 개념 3.시스템의 정적인 모습을 나타냄	연관관계(집합, 복합,의존) 정의
Requirement Diagram	1.요구사항 정의에 대한 표현 2.요구사항과 이 요구사항을 다른 모델링 엘리먼트와 연결할 수 있는 모델 엘리먼트를 제공 3.원 요구사항으로부터 파생 또는 유도되는 요구사항을 표현가능. 4.요구사항의 충족관계를 표현 가능 5.Test Case를 통한 검증가능	요구사항 정의 요구사항 추적성 정의
Parametric diagram	파라메트릭 다이어그램은 어셈블리를 이용하여 시스템의 성능 및 신뢰성 등의 분석을 할 수 있도록 하기 위한 다이어그램. 모델하는 시스템의 물리적 특성을 수식표현 성능상 중요한 파라미터를 특정하는 등의 분석을 행하는 것이 가능	제약사항 정의



<Figure 3> A representation of the interface data model in terms of data model classes

3. 구현

3.1 SysML을 통한 통합설계프로세스 모델의 구현

본 연구진의 선행연구 [4],[5]를 통한 제시한 연구결과를 <Figure 3>과 같으며, 제시된 기존의 연구결과를 바탕으로 SysML 구현을 위한 방안을 제시하였다. 상위의 연구활동을 통해 SysML의 특성에 대해서 분석 되었다. 따라서, 기존의 제시한 통합 프로세스 모델에서 제시된 개별적 활동 및 산출물의 특성을 분석하여 SysML을 통해 대체 가능한 활동을 정의하였다.

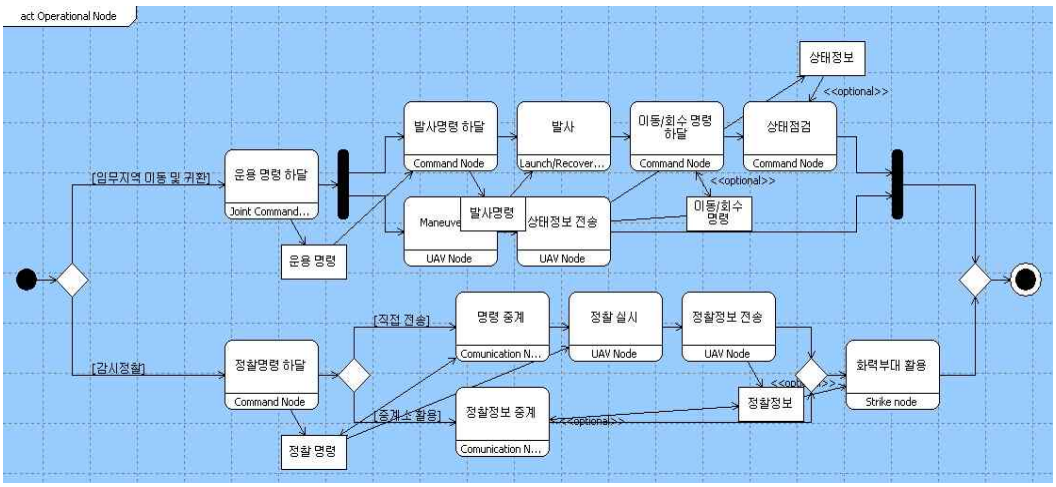
시스템공학의 설계 프로세스는 크게 4가지 단계로 구성된다[6]. 우선, 첫 번째로 행하는 단계는 요구사항을 생성하는 단계이다. 본 단계에서는 이해당사자로부터 수집된 정보를 바탕으로 생성된 요구사항 또는 생성 근거를 위한 자료를 바탕으로 Requirement Diagram을 통해서 생성 및 관리하게 된다. 또한, 이를 통해 생성된 요구사항을 바탕으로 시스템 안전계획에 반영되어야 할 것이다.

시스템공학 설계 프로세스에 따른 두 번째 단계는 첫 번째, 요구사항 생성과정을 통해 생성된 요구사항을 바탕으로 이해당사자 요구사항을 시스템요구사항으로 전환하는 단계로서 유스케이스 다이어그램(Usecase Diagram)의 활용을 통해서 시스템이 수행해야하는 주요 임무를 기능 중심으로 식별이 가능하다. 또한, 이러한 유스케이스 다이어그램(Usecase Diagram)을 통해 상위레벨의 시스템이 지녀야할 안전 분석이 가능하므로 PHL(Preliminary hazard list) 및 PHA(Preliminary hazard analysis)에 대한 대체 활동으로 가능해진다.

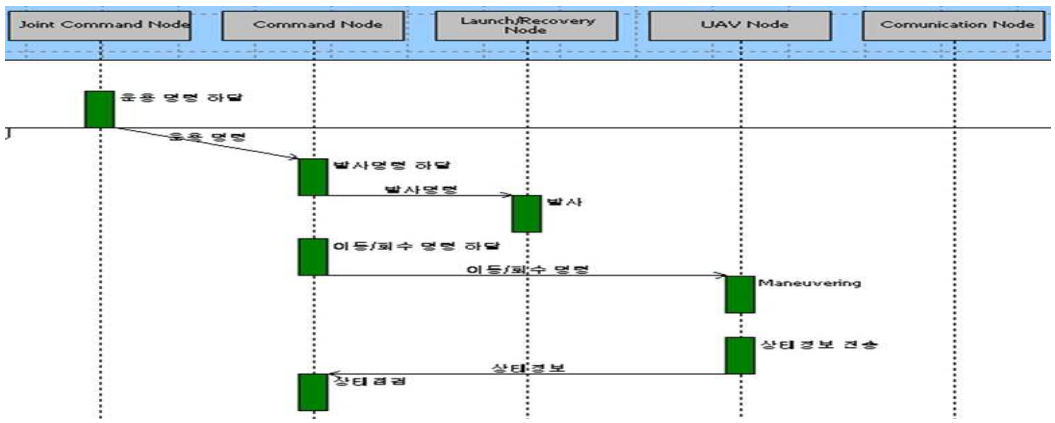
시스템공학 설계프로세스에 따른 세 번째 수행단계는 기능분석단계이다. 본 단계에서는 개발하려고 하는 시스템이 지녀야할 기능을 상위레벨에서 하위레벨로 분해하는

단계로서 이 단계에서는 Activity Diagram, Block Definition Diagram, 시퀀스 다이어그램을 통해서 기능분석 활동을 나타낼수 있다. 또한 이러한 다이어그램을 통해서 상위레벨에서의 FHA 및 SHA를 수행하는데 있어서 대체 가능한 역할을 할 수 있을 것으로 기대된다. 또한, 기능분석 단계를 도출된 시스템 분해구조(SBS, System Breakdown Structure)를 도출 할 수 있다. 이렇게 구조화된 시스템분해구조를 바탕으로 기능할당 단계에서 거동분석을 통해 도출된 하부 요구사항에 할당하면 되겠다.

시스템공학 설계 프로세스의 네 번째 단계에 해당하는 기능할당에서는 이전 기능분석 활동을 통해 분해된 기능을 시스템 구성 컴퍼넌트에 할당하는 활동을 말한다. 이렇게 할당된 기능들은 어떠한 흐름으로 진행되는지 <Figure 5>와 같은 시퀀스 다이어그램(Sequence Diagram)을 통해서 표현가능하다.

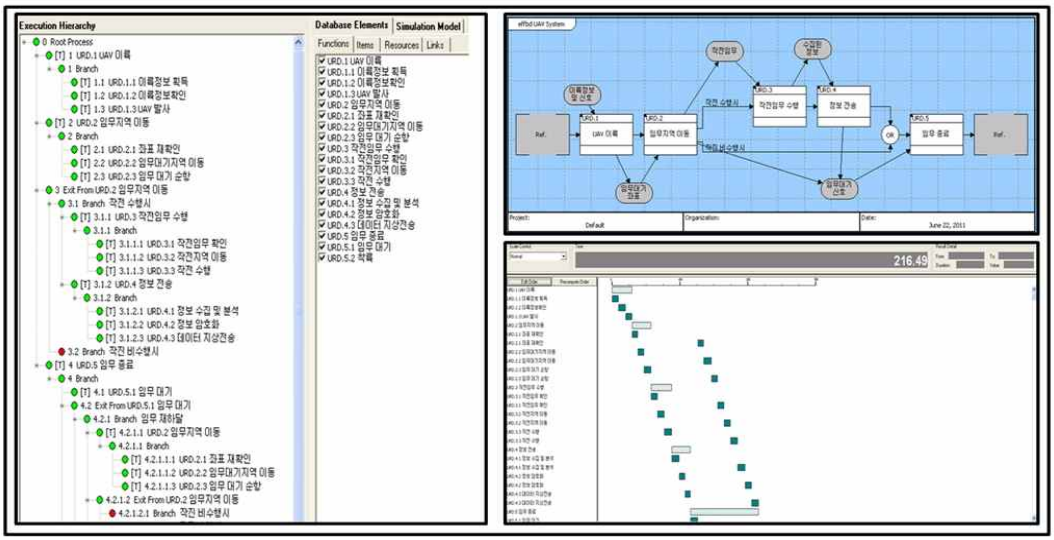


<Figure 4> Operation of UAV System_Activity Diagram



<Figure 5> Operation of UAV System_Sequence Diagram

마지막으로 시스템공학 설계프로세스의 마지막 단계인 설계통합 단계이다. 이 단계에서는 물리적 아키텍처 구성요소에 할당된 기능들이 만족하는지에 대한 설계 대안들이 검토 및 결정되는 단계이다. 따라서, 최종적으로 시스템 요소가 정의된다. 앞에 수행한 기능 분석 및 할당이 완료되고 하부 시스템의 대안이 최종 아키텍처로 선택되면 Internal Block Diagram을 통해서 하부 시스템의 구성, 물리적 인터페이스 등을 정의하게 된다. 최종적으로 IBD를 통해, 물리적 설계에 대한 검증을 수행할 수 있다.



<Figure 6> Verification of the resultant UAV design by computer simulation

3.2 시스템공학 전산지원 도구를 통한 구현 결과의 검증

본 연구의 대상인 통합 설계프로세스 모델을 검증하기 위해 무인항공기 시스템에 적용하여 Case Study를 수행하였다. 따라서, 대상 시스템인 개념설계 단계의 군사용 무인항공기 체계에 SysML 적용을 통한 모델기반 설계접근을 시스템공학 전산지원 도구인 CORE를[7] 통해 구현하였다. 개념설계 단계의 무인항공기의 SysML 적용을 검증하기 위해, <Figure 6>과 같이 CORE 툴의 검증 가능한 모델링 기법인 EFFBD를 통해 Time-Line analysis을 통한 시뮬레이션을 수행하였다. Time-Line analysis을 통해 EFFBD 모델의 논리적 오류를 발견하고 개선하는 과정의 반복을 통해 모델링 과정에 대한 개선을 할 수 있었으며 “Unaddressed Leaf-Level Requirements Query” 보고서 출력을 통해 개념설계 단계 과정에 반영되지 않은 활동들을 정렬할 수 있었다. 이밖에 CORE 툴이 지니고 있는 추적성 특성에 의해 개념설계 단계의 시스템 개발과정에 있어서 이후 변경내용 따른 변경된 사항에 대한 추적관리 또한 가능하다.

4. 결론 및 향후 연구 방향

각계 산업분야의 고도화된 기술의 발전으로 인해 인류는 보다 인간에게 편의를 제공하기 위해 지속적 발전과정을 거치며 시스템을 개발해왔다. 물론, 이에 따른 큰 효용성을 인간에게 안겨다 주었다. 하지만, 최근 대형 복합 안전중시 시스템을 중심으로 수많은 사고들이 국제적으로 발생하다 보니, 체계적인 설계 접근법과 안전성 확보에 대해 이슈로 떠오르고 있다. 본 연구진은 이러한 국제적 추세에 앞서 다년간 시스템 상위 레벨에서의 시스템 설계 활동과 시스템 안전활동의 상호운용성에 대한 연구를 바탕으로 통합된 설계 프로세스 모델을 제시하였었다. 따라서, 이러한 연구결과를 시스템 개발에 연관된 모든 이해당사자들이 공통된 인식 및 상호연동성에 대한 이해가 밑바탕으로 전제되기 위해 본 연구를 통해 방안을 제시하였다. 따라서, 모델기반 시스템공학 기법중 하나인 SysML을 통해 시스템 설계 과정에서 표준 언어로서 역할을 하는 방법론을 가지고 통합 프로세스 모델을 구현하기 위한 연구를 수행하였다. 본 연구수행을 통해 시스템설계 프로세스와 시스템 안전활동에 해당하는 개별 활동에 대한 특성을 분석하였으며, 또한 이러한 활동을 SysML을 통해 표현·구현하기 위한 SysML이 지니고 있는 개별 특성에 대해 분석하였다. 또한, 이러한 분석된 결과를 바탕으로 SysML을 통한 시스템설계 및 시스템 안전활동을 구현하기 위한 발판을 마련하였다. 본 연구결과를 추후 활용측면에서 높이기 위해, 본 연구가 개념설계 단계에서 주된 초점을 두었다면, 보다 확장된 수명주기를 대상으로 연구를 수행한다면 보다 가치 있는 연구가 될 것으로 기대된다.

5. 참 고 문 헌

[1] J. C. Knight, “Safety critical systems: challenges and directions”, in Proc. 2002. ICSE, Orlanda, USA, 3-10, May, (2002)

[2] A. E. Clifton, “Hazard analysis techniques for system safety.”, Hoboken, New Jersey: John Wiley & Sons, Inc., (2005)

[3] www.omgsysml.org

[4] Y. M. Kim and J. C. Lee, “A Study on the Integration of Systems Engineering Process and Systems Safety Process in the Conceptual Design Stage to Improve Systems Safety,” Korea Safety Management & Science, vol. 14, pp. 1-10, (2012)

[5] Y. M. Kim and J. C. Lee, “On the Integration of Systems Design and Systems Safety Process from an Integrated Data Model Viewpoint,” Korea Safety Management & Science, vol. 14, pp. 107-116, (2012)

[6] A. Kossiakoff and W. N. Sweet, Systems Engineering Principles and Practice. New Jersey: Wiley, 2003, pp. 117-138.

[7] www.vitechcorp.com/