J. Korea Saf. Manag. Sci. Vol. 15 No. 3 September 2013
http://dx.doi.org/10.12812/ksms.2013.15.3.7

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

안전중시 시스템의 설계프로세스 구축에서 SysML 모델의 활용에 관한 연구

김 영 민* · 이 재 천*
*아주대학교 시스템공학과

On the Use of SysML Models in the Construction of the Design Process for Safety-Critical Systems

Young Min Kim* · Jae-Chon Lee*
*Dept. of Systems Engineering, Ajou University

Abstract

The recent trend in modern systems development can be characterized by the increasing complexity in terms of both the functionality and HW/SW scale that seems to be accelerated by the growing user requirements and the rapid advancement of technology. Among the issues of complexity, the one related to systems safety has attracted great deal of attention lately in the development of the products ranging from mass-transportation systems to defence weapon systems. As such, the incorporation of safety requirements in systems development is becoming more important. Note, however, that since such safety-critical systems are usually complex to develop, a lot of organizations and thus, engineers should participate in the development. In general, there seems to be a variety of differences in both the breadth and depth of the technical background they own. To address the problems, at first this paper presents an effective design process for safety-critical systems, which is intended to meet both the systems design and safety requirements. The result is then advanced to obtain the models utilizing the systems modeling language (SysML) that is a de facto industry standard. The use of SysML can facilitate the construction of the integrated process and also foster active communication among many participants of diverse technical backgrounds. As a case study, the model-based development of high-speed trains is discussed.

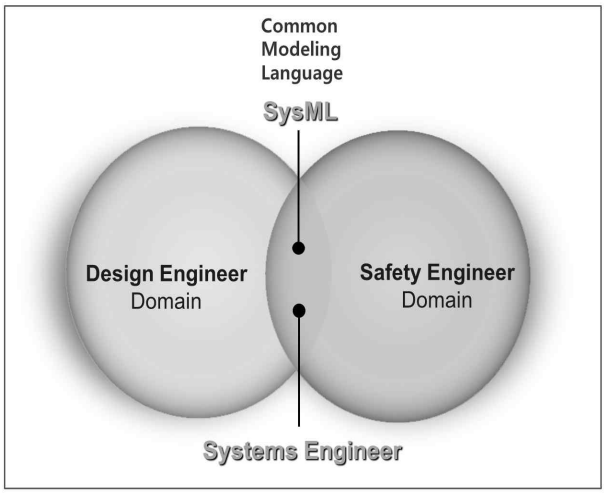
Keywords: Safety-Critical Systems, SysML, Model-Based Approach, Conceptual Design, Safety

† 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구 사업임 (No. NRF-2012R1A1A2009193)

† Corresponding author: Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, Wonchon-dong, Youngtong-gu, Suwon, 443-749. Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received July 19, 2013; Revision Received Sept. 3, 2013; Accepted August. 27, 2013.

1. 서 론

오늘날 개발되는 대형 복합 시스템을 중심으로 시스템의 설계단계 뿐만 아니라 운용 및 유지보수, 폐기 단계에 이르기까지의 시스템 전 수명주기 관점에서 시스템의 안전성 확보에 대한 노력을 기울이고 있는 추세이다[1]. 하지만 대부분의 대형복합 시스템의 개발환경에서 시스템 설계와 시스템 안전이 사실상 독자적인 영역으로 취급되고, 활동되다 보니 최근과 같이, 시스템 설계 단계에서 시스템 안전성 확보에 대한 중요성을 인지하면서도 사실상 접근함에 있어서 상당한 어려움을 겪고 있다[2]. 또한, 시스템 설계와 안전 확보를 위해 종사하는 개별적 분야의 엔지니어는 서로 상이한 모델링 기법과 문법을 사용함에 따라 엔지니어 사이에서 의사소통과 그에 따른 문제 유발로 개발 지연 및 비용 상승을 초래해왔다[3].



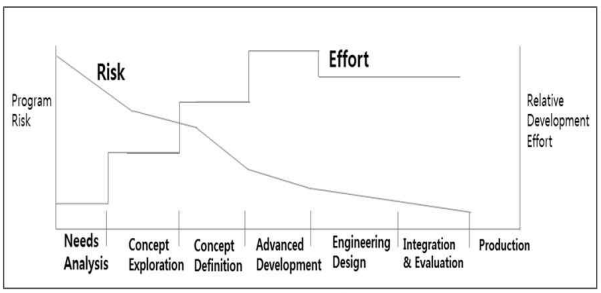
<Figure 1> The role of SysML between design engineer and safety engineer.

따라서, 이러한 문제점을 해결하고자, 2006년 INCOSE와 OMG의 협력으로 SysML이 개발되었다. SysML은 기존의 소프트웨어 개발에서 널리 사용되어왔던 UML과 상당히 유사 하지만, UML이 소프트웨어 중심의 개발에서 사용되어왔다면, SysML은 시스템 설계를 위한 구현과 모델링을 수행함에 있어서 시스템의 사양화, 거동분석, 설계, 논리적 타당성 확인 및 검증을 수행하기 위해 이용될 수 있어, 오늘날 국방, 우주항공, 자동차 개발 분야에서 폭넓게 이용되어 지고 있다[4].

오늘날 개발되는 시스템은 과거의 일반적인 운용측면만 고려되었던 시스템과 달리, 상당수 시스템은 안전성 측면에서 중요도를 내포한 특성을 지닌, 안전 중시 시스템(Safety-Critical System)이라 볼 수 있다. 그럼에도 불구하고, 오늘날 설계단계에서 안전성을 고려한 동시 공학적(Concurrent Engineering)인 접근에 관한 연구가 부족하다 보니 방법론 등 많은 부분에서 부족한 실정이다.

따라서, 본 연구는 안전중시 복합 시스템의 개념 설계단계에서부터 안전성 확보를 위해 설계 프로세스에 안전성을 고려한 하나의 통합 프레임을 제안하였다. 또한, 제안된 통합 프레임을 SysML로 표현하기 위해, 통합 프레임과 SysML이 지니고 있는 특성을 분석하여 국내 안전중시 대형복합 시스템을 개발하는데 있어서 실질적 방안을 제시하고 사례분석을 통해 개선된 방법론에 대한 평가를 수행하였다.

최근 들어, 자동차 산업분야에서 차량이 기존의 하드웨어 중심의 발전을 이루다 오늘날 소프트웨어 중심의 성장에 초점을 두고 있다. 이에 따라, 기능중심의 안전도 향상이 중요시 여기게 되다보니, 이전의 상세설계 단계에 중점을 두었던 설계 및 안전 활동이 보다 초기단계인 개념설계 단계로 전이되는 양상을 보이고 있다. 이러한 노력은 또한, 최근 제정된 ISO 26262[4]를 통해서도 엿볼 수 있는 대목이다.

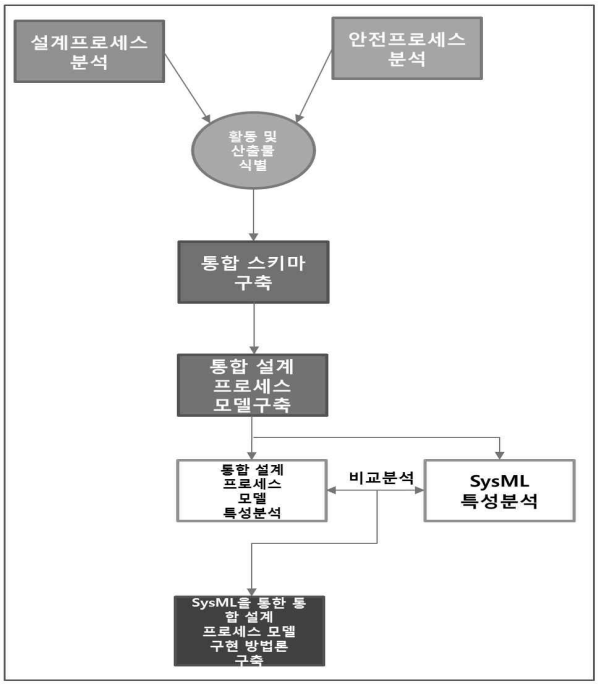


Phase / Level	Needs Analysis	Concept Exploration	Concept Definition	Advanced Development	Engineering Design	Integration & Evaluation
System	Define Operational objectives	Explore Concept	Define Selected concept			
Sub-System		Define Function	Define configuration			
Component			Select Define functions			

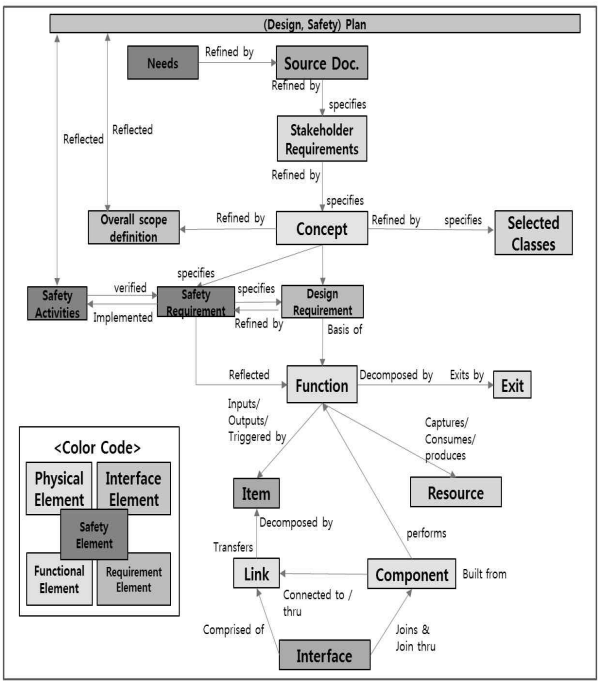
<Figure 2> The importance of safety in the conceptual design phase[5].

이러한 맥락에서, 시스템 설계 프로세스와 시스템 안전 활동의 통합에 관한 연구가 선행연구[5],[6],[7]을 통해 발표되었다.

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



<Figure 3> A conceptual diagram representing the objectives of the paper.



<Figure 4> Designed schema to reflect the safety

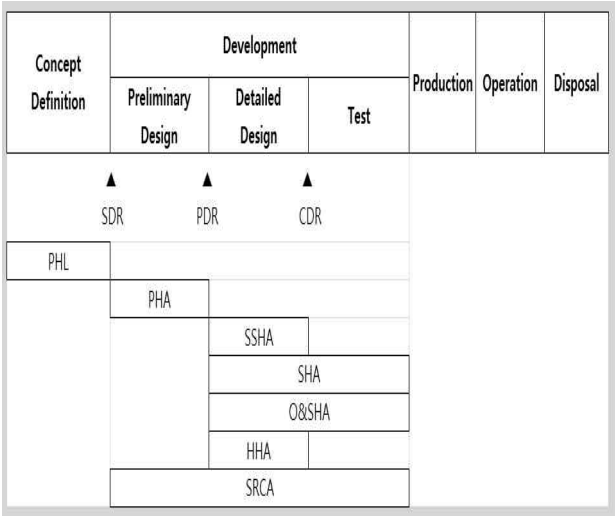
선행연구 [5]에서는 시스템공학 설계 프로세스와 시스템 안전 활동과 통합에 관한 연구를 수행하였다. 또한, 서로 다른 학제간 프로세스 통합을 제시함에 따라, 서로 다른 영역에서 활동하는 엔지니어로 하여금 공통의 언어로서 제시하지 못했다는 점에서 관련 엔지니어로 하여금 혼동을 줄 수 있다. 선행연구 [6]에서도 같은 맥락에서 프로세스 통합에 관한 연구를 수행하였지만, 통합된 프로세스에서 수행해야할 안전 활동의 수행 순서에 관해 제시하지 못하고 있다. 선행연구[2]에서는 설계단계에서 SysML의 유용성을 인지하고, 이를 활용한 복합 시스템의 신뢰성 향상 방안에 관해 다루고 있다. SysML으로 시스템 설계를 수행하고 해당 논문에서 제시하는 다른 툴로 SysML을 통한 모델링 결과가 자동 변환 될 수 있도록 위험원분석 기법의 특성을 반영한 알고리즘을 개발하는데 초점을 두고 있다. 따라서, 본 논문에서 주장하는 시스템 설계의 상위 수준인 개념설계 단계에서 안전성 확보를 위한 방안으로 설계와 안전활동 프로세스 간에 통합을 실시하고, 두 학제가 동일한 이해를 갖을 수 있도록 SysML을 통해 통합 프로세스 모델을 구현하는 방안을 제시하고 있다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 언급하였다. 3장에서는 개념설계단계에서 안전성을 고려한 통합 프레임을 확립한다. 4장에서는 제시된 통합 프레임을 SysML과 상호분석을 통해 연동성을 제시하였다. 마지막, 5장에서는 SysML을 통해 구축된 통합 설계 프레임을 바탕으로 CASE STUDY의 적용을 통해 본 논문 주장에 대한 결과를 정리 및 요약 하였다.

2. 문제의 정의

2.1 SysML 접근을 통한 시스템 설계 및 안전 활동의 필요성

국내에서도 모델기반 기법을 통한 설계적용에 관한 연구는 상당 시간동안 이루어져 왔다. 하지만, 본 논문에서 적용한 SysML을 통해 시스템 설계 단계와 안전 활동에 대한 대체기법에 대한 연구 활용에 관한 연구가 활발한 국제적 추세에 있음에도 불구하고 아직 국내 개발환경에서는 필요성 부족이라는 인식의 부재로 인해, 연구에 대해 미흡한 실정이다. 최근 국제적으로 대형 복합 시스템으로부터의 잇따른 사고로 인해, 안전성 확



<Figure 5> The main safety activities in the design phase[1].

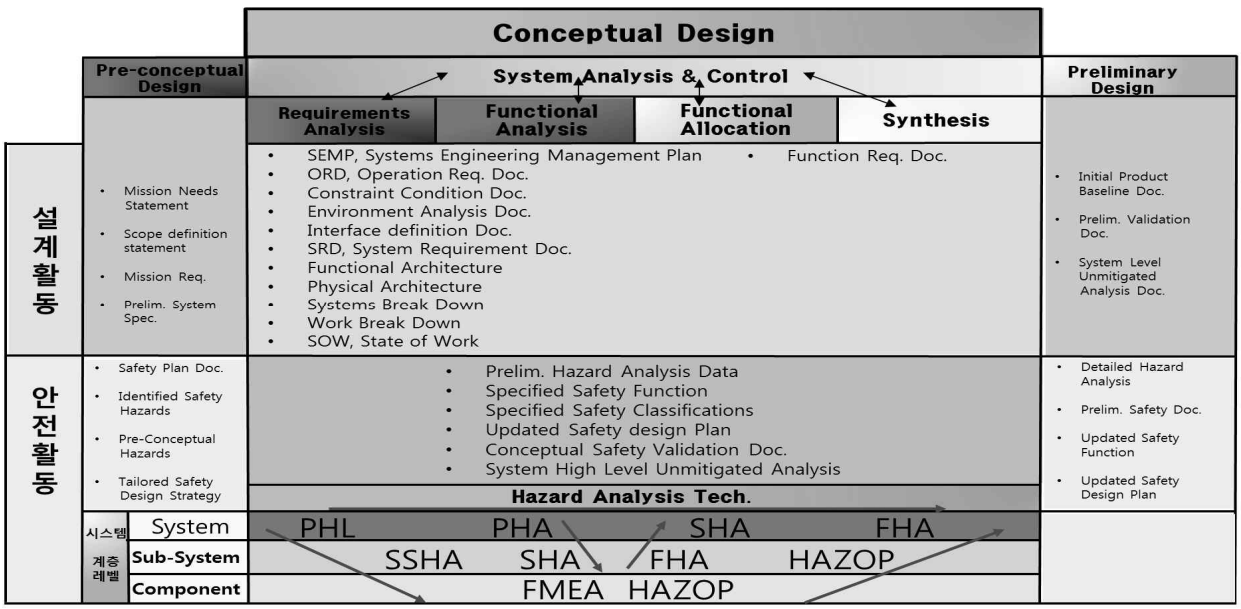
보에 대해 어느 때 보다 중요하게 인지하고 있다. 따라서, 본 연구의 수행을 통해 시스템 설계프로세스에 시스템 안전 활동과 통합의 필요성을 적시하고 연구되어야함을 주장한다.

특히, 본 연구의 수행을 통해, <Figure 1>에서 제시하는 바와 같이, 시스템 설계 영역과 시스템 안전 활동의 영역의 공통기법의 역할이 가능한 SysML의 분석을 통한 설계프로세스와 안전성 활동과의 상호연계성 제공을 통해서 타 전문영역간 가교 역할 수행이 가능해질 수 있을 것으로 기대된다. 또한, 본 연구 수행을 통해 제안되는 시스템설계와 시스템안전 활동 사이에 공통된 모델링 기법으로 두 활동 사이에 유기적인 흐름을 제공함으로써 개별 도메인 엔지니어로 하여금 실질적 활용 가치를 높일 수 있을 것으로 기대된다.

2.2 개념설계 단계에서의 안전성에 대한 연계 확립성의 필요성

<Figure 2>에서 제시하는 시스템 설계 수명주기 상에 개념설계 단계는 수명주기의 첫 단추 역할로 설계의 기본을 세우는 과정이다. 지금의 안전 활동들은 대체로 상세설계 단계 또는 설계 종료 시점 이후의 안전 활동에 주된 초점을 맞추고 있다. 따라서, 지금의 접근 방식에서 벗어나, 초기 설계단계에서 위험원 식별 및 위험평가를 반영함으로써, 설계변경에 따른 상당한 비용을 줄일 수 있어, 시스템 및 기타 제품의 생산함에 있어 마켓으로의 지연시간과 개발 비용을 절감할 수 있다[7].

또한, 오늘날 시스템 설계단계의 안전 활동이 시스템의 기능을 중심으로 이뤄지고 있다. 특히, 시스템 설계에서 기능이라는 것은 시스템 요구사항을 기반으로 생성되는 것이기 때문에, 개념설계 단계의 요구사항 개발단계로부터 안전 활동과 연계성을 갖고 연구함으로써 안전성 확보에 대해 보다 할 걸음 나아갈 수 있을 것이다.



<Figure 6> The system design process and system safety activities performed in accordance with the process output[9].

2.3 연구 목표 및 방법

상위 선행연구 분석을 통해 본 논문에서 대상으로 다루려고 하는 안전중시 시스템이 설계 단계에서 안전성 확보에 대한 노력이 필요하며, 시스템 설계 엔지니어와 안전성 확보를 노력 하는 엔지니어 사이에서 원활한 커뮤니케이션을 위해 SysML이라는 공통의 언어의 필요성에 대해서 인지하였다.

본 연구에서는 이를 위해 시스템공학 국제 설계 표준인 EIA-632[8]와 안전표준인 MIL-Std.-882d[9]를 기반으로 개념설계 단계에서 시스템 안전을 동시에 고려한 통합 프레임 워크를 제안하였다.

제안된 통합 프레임워크를 본 연구에서 모델기반 접근 방법 중 하나로 활용한 SysML을 바탕으로 시스템 설계와 안전 활동이 이행 가능하도록 논리적 근거를 제공하였다. 통합 프레임워크를 바탕으로 CASE STUDY 적용을 통해 본 연구의 주장에 대한 검증을 수행하였다. 또한, 통합 프로세스 모델 구축에 따른 SysML 적용에 관한 연구 방법을 <Figure 3>을 통해서 도식화 하였다.

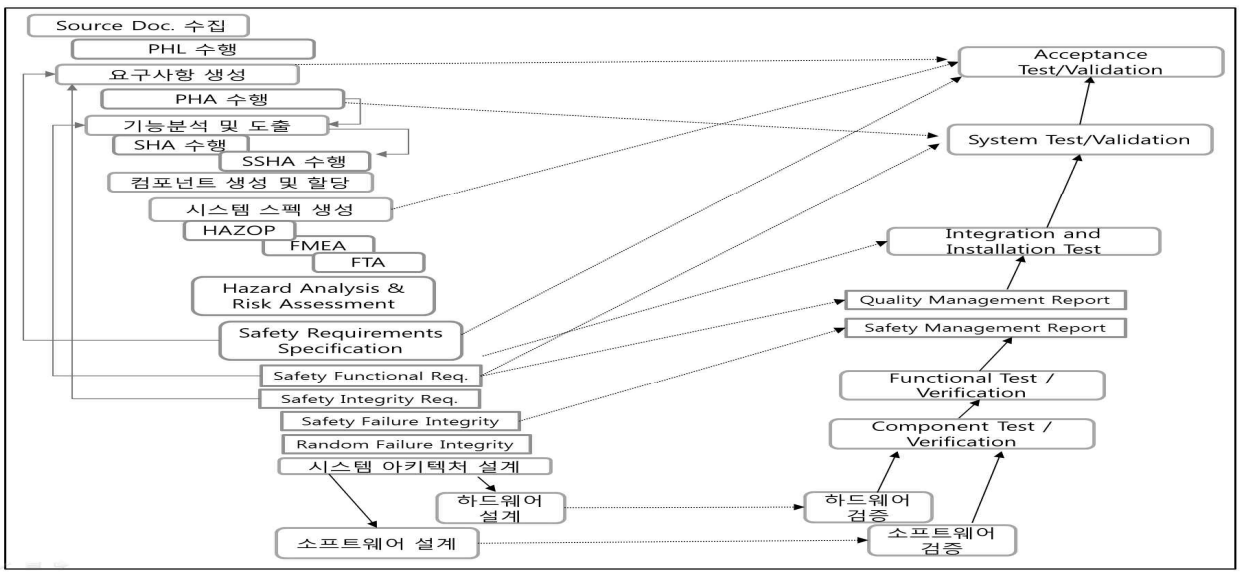
3. 안전성을 고려한 통합 시스템 설계 프레임 구축 활동

3.1 개념설계 단계의 설계 및 안전 활동과 입·출력 산출물 분석

시스템의 설계단계를 참고문헌[10]에서는 Concept Development, Engineering Design, Post Engineering이라는 3단계로 규정하고 있다. 이 중 개념 설계 단계는 첫 번째 해당하는 단계로서, 개념 설계 단계란 시스템 설계 프로세스 초기의 한 부분으로서 사용자가 요구사항을 개념적 모델로 변환하는 단계로 바라보고 있다. 이러한, 개념설계 단계의 하위 프로세스는 크게 5가지로 구성된다[11]. 구성은 아래와 같다.

1) 이해당사자 요구사항 정의 및 분석
2) 기능분석
3) 설계조합
4) 검증(Verification)
5) 확인(Validation)

위 <Figure 4>을 통해서 알 수 있듯이, 시스템 설계와 안전 활동과 그에 따른 산출물들 간의 상호 관계를 스키마(Schema)를 통해 정립하였다. 제안한 스키마는 일반적 설계단계에서 안전성 반영위해 반영할 수 있는 안전속성을 지닌 계획, 활동, 산출물을 중심으로 기존 설계관점의 스키마를 보완하여 생성하였다. 생성된 스키마는 이후 통합 프레임을 생성하는데 있어서 설계와 안전 활동 간의 상호 연동성을 분석하는데 있어서 중요한 근거 자료로서 활용하였다.



<Figure 7> Integrated vee process model.

<Table 1> The general characteristics of SysML Diagrams.

주요 특성	SysML Diagram	일반적 특성
구조	Block Definition Diagram(BDD)	SysML에 있어서 Block은 시스템과 그 구성요소를 표현하는 단위로서 BDD는 Block과 Block 간 관계를 정의하기 위한 다이어그램 이다. BDD를 사용하는 것으로서 Block에 의해 본질적인 부분에 주목한 추상도 높은 분석을 수행할 수 있다.
	Internal Block Diagram(IBD)	내부구조를 표현하기 위한 다이어그램으로서, 어떤 Block이 별도의 종류의 Block군으로부터 구성되는 것을 나타낼 수 있다.
	Parametric Diagram(PD)	시스템에 표현되는 다양한 값 사이에 성립되는 제약을 수식 등을 사용해서 표현하기 위한 다이어그램 이다. 파라미터 다이어그램을 사용해서 성능 상 중요한 파라미터를 특정하는 등의 분석을 수행하는 것이 가능하다.
	Package Diagram(PKD)	Block 등의 모델 요소군을 그룹화하기 모델 요소로서 Package나 Package 간의 관계를 표현하기 위한 다이어그램.
동적	Activity Diagram(AD)	작업이나 처리가 어떤 순서로 진행되는지, 어떠한 조건에서 처리가 실행되는가에 대해서 거동을 분석함으로서 다양한 시점을 진행하고 유용한 정보를 얻을 수 있다.
	Sequence Diagram(SD)	모델 요소간의 상호작용을 시간적으로 표현하는 것으로서 모델 요소의 협조에 의해 실현되는 거동을 표현하기 위한 다이어그램.
	State Chart Diagram(SCD)	Block 등이 가지고 있는 상태나 상태전이의 방법을 표현하기 위한 다이어그램.
	UseCase Diagram(UCD)	시스템의 기능이나 시스템이 지니고 있는 기능과 시스템 사용자 간의 관계를 나타냄.
요구사항	Requirements Diagram(RD)	시스템이 만족해야하는 요구사항이나 요구사항 간에 관계를 표현하기 위한 다이어그램이다. 요구사항 다이어그램에 등록할 요구사항을 다른 다이어그램에도 표기하고 다른 모델요소와의 관계를 표현하는 것으로서 요구사항 간 에 추적성을 명확하게 할 수 있다.

3.2 식별된 활동 및 산출물의 특성 및 속성 분석

설계단계의 활동과 산출물을 중심으로 우선 설명하자면, 설계단계의 첫 활동은 개발에 관련한 이해당사자로 하여금 요구사항 수집으로부터 시작 한다. 이러한 활동을 시작으로 비공학적 기술사항이 공학적 산출물로 변모하는 과정을 거치게 된다. 요구사항 개발과정을 거쳐 이해당사자로 하여금 요구사항을 식별하고 개발 범위를 명확히 하여 설계 대상이 되는 시스템을 설계하는데 목표를 분명히 하는데 목적이 있다. 요구사항 정의 및 분석 프로세스를 통해서, 개발 대상에 대한 시스템 운용요구사항, 시스템요구사항, 제약요구사항, 환경요구사항 등이 개발되게 된다. 특히, 이후 이러한, 이해당사자 요구사항 정의로부터의 산출물을 바탕으로 기능분석 단계를 거치기 때문에, 오늘날 안전공학 분야에서 우선적으로 다루어 안전성 확보를 위해 노력하는 부분이기에 초기 개념설계단계의 노력으로 기능안전, 시스템 환경 안전성 확보를 통해 시스템 안전성을 확보하는 방안중 하나가 될 수 있다. 요구사항 개발프로세스 거쳐 생성된 산출물은 기능분석 프로세스의 입력자료로서 활용되어 시스템 요구사항을 바탕으로 이를 기능적으로 이행하기 위한 요구사항이 개발되게 된다. 이러한 요구사항은 시스템 안전성에 직접적인 영향을 미칠 수 있기 때문에 특히, 기능요구사항 개발단계에서 보다 안전 활동에 대한 노력이 필요하다. <Figure 6>에서도 제시하듯이, 본 연구팀은 기존 연구를 통해, 시스템 설계 수명주기 상에 시스템 계층에 따른 시스템 안전 활동을 정의 하였다. 하지만, 이러한 결과는 설계프로세스와 안전 활동을 수행하는데 있어서 연속적인 수행 근거를 제공하지 못한다. <Figure 6>을 통해서 식별되었듯이, 개념설계 단계에서 필요한 안전 활동을 다음과 같이 정의하였다[6].

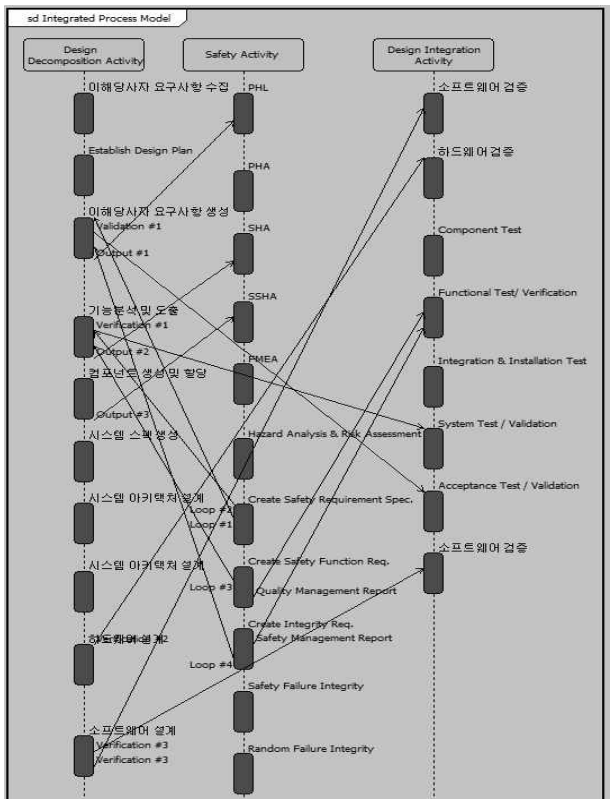
1) System Safety Program Plan(SSPP)
2) Preliminary Hazard List(PHL)
3) Preliminary Hazard Analysis(PHA)
4) Subsystem Hazard Analysis(SSHA)
5) System Hazard Analysis(SHA)

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

이렇게 규정한 이유는 개념설계 단계를 거쳐 시스템의 본질을 정의하게 되고, 시스템의 최하부까지 설계와 안전 활동을 수행하는 것이 아니라 시스템, 서브-시스템, 컴포넌트 수준까지의 레벨을 개념설계에서 수행하기 때문이다. 따라서, 설계단계에서의 안전 활동 역시 동수준에서 수행 가능한 활동들이 이행되어져야 한다.

3.3 안전성을 반영한 통합 설계 프로세스 모델 구축

<Figure 7>에서 제시하는 통합 시스템 설계 프로세스 모델은 앞서 분석된 개념설계 단계에서의 설계활동과 산출물 그리고, 시스템 안전 활동과 산출물에 대한 특성 분석을 수행한 결과를 활용하였다. 따라서, 이러한 결과를 바탕으로 상호 프로세스 간에 연계성을 고려하여 연속적인 프로세스로 활용될 수 있도록 통합적 관점에서 제시하였다.



<Figure 8> Establishing integrated process model using CASE Tool.

다음은 통합 설계 프로세스 모델에 대해 기술하겠다. 현대의 시스템 개발과정에서 새롭게 개발되어 물리적 구현되는 시스템은 극히 드물 것 이다. 따라서, 기존 시스템(Legacy System)과 엔지니어의 경험을 바탕으로 시스템 설계와 안전에 관한 전체적인 계획을 세우고, 설계의 진행상황에 따라 다시 계획에 반영되어 지속적인 조정이 이루어 진 다는 것을 <Figure 4>의 스키마를 통해 알 수 있다.

따라서, 통합 설계 모델은 시스템 개발 계획 수립을 시작으로 하여, 요구사항 개발을 위해 이해당사자로 하여금 요구(Needs)를 수집하게 된다.

수집된 요구를 정제하여 이해당사자 요구사항이 생성된다. 생성된 이해당사자 요구사항은 시스템의 최상위 수준에서의 내용을 담고 있기 때문에, 안전 활동인 PHL을 수행하는데 중요한 정보를 제공한다. PHL은 대상 시스템에 대한 상위 수준에서 위험원을 정의하며, 수행의 목적은 시스템 위험원에 대한 초기 식별이라고 할 수 있다.

기능요구사항 개발단계는 개발 대상 시스템의 운용개념 및 시스템 개념을 통해 생성된다. 따라서, 개념설계라는 상위 수준에서의 설계활동을 통해 기능요구사항이 개발되기 때문에 앞서 정의한 대로, 시스템, 서브-시스템, 컴포넌트 수준의 기능의 흐름 분석을 통해, 각각의 수준에서 이행해야 할 요구사항을 식별하게 된다. 그러므로, 본 단계에서는 PHA가 수행되어야 한다. PHA는 개발의 초기단계의 시스템 레벨에서 위험을 식별하기 위한 상위 수준에서의 예비활동이다. 서두에 언급대로, 안전공학 분야에서 최근 시스템 안전성 확보를 위한 방안중 상당수가 기능중심으로부터 발생되기 때문이다. 이후의 설계단계에서는 SHA와 SSHA의 안전 활동이 수행될 것이다. 특히, 기존의 안전공학분야에서는 시스템 안전 확보를 위해 수행하는데 있어서 상향식 접근(Down-Top)으로 접근을 해왔기 때문에, SSHA가 먼저 수행되고, 이후, SHA를 수행되어왔다. 하지만, 설계프로세스와 같은 하향식 접근(Top-down) 접근을 통해, 두 프로세스 간에 병행 측면에서 보다 유용하게 접근 가능하다. 시스템 상위수준의 포괄적 접근에서 세부적으로 하향식 접근을 통해, 안전성 확보에 대한 총체적 관점에서 접근이 가능해 진다.

SHA는 시스템 사양에 포함된 안전 요구사항을 준수하는지 시스템을 검증하기 위해서 수행, 서브-시스템 인터페이스와 시스템 기능 오류와의 연관된 식별되지 않은 위험원을 인지하는 활동이다. 또한, SHA를 수행하기 위해서 수반되는 위험분석 기법으로는 다음과 같다[3].

1) FTA(Fault Tree Analysis)
2) FMEA(Failure mode and effects analysis)
3) ETA(Event tree analysis)
4) Interface Analysis

위 4가지 기법은 기능을 중심으로 수행되기 때문에 SHA 역시, 기능 분석 및 도출 단계를 거쳐, 이후에 이행되어 설계 산출물을 활용해야 할 것이다.

SSHA는 서브-시스템에 포함된 안전요구사항을 서브-시스템이 준수하는지를 검증하기 위해 SSHA를 수행하며 서브-시스템의 설계와 연관된 알지 못하는 위험원을 조기 식별하기 위해 수행한다. 따라서, SSHA는 서브-시스템 수준의 활동에 중점을 두고 있다. 설계단계에서 시스템의 물리적 구성 및 시스템 레벨을 명확히 정의하기 위해서는 개념설계 단계의 세 번째, 프로세스인 컴포넌트 생성 및 할당 단계가 필수 전제되어야 된다. 생성된 기능요구사항은 컴포넌트에 할당되기 때문에 기능오류로 인해 컴포넌트에 미치는 영향도 분석 또한 가능해 진다.

또한, <Figure 7>을 통해서, 알 수 있지만, 생성된 안전요구사항과, 위험원 분석 활동 결과는 설계단계 재반영 될 수 있도록 Loop 형태의 반복적인 수행이 진행된다는 것을 나타낸다.

4. SysML 기반 프로세스 모델 환경구축

4.1 SysML의 특성 분석

SysML은 크게 3가지 특성을 지닌 다이어그램으로 구성되어 있으며, 구조와 거동 그리고 요구사항을 나타내는 다이어그램으로 구성된다.

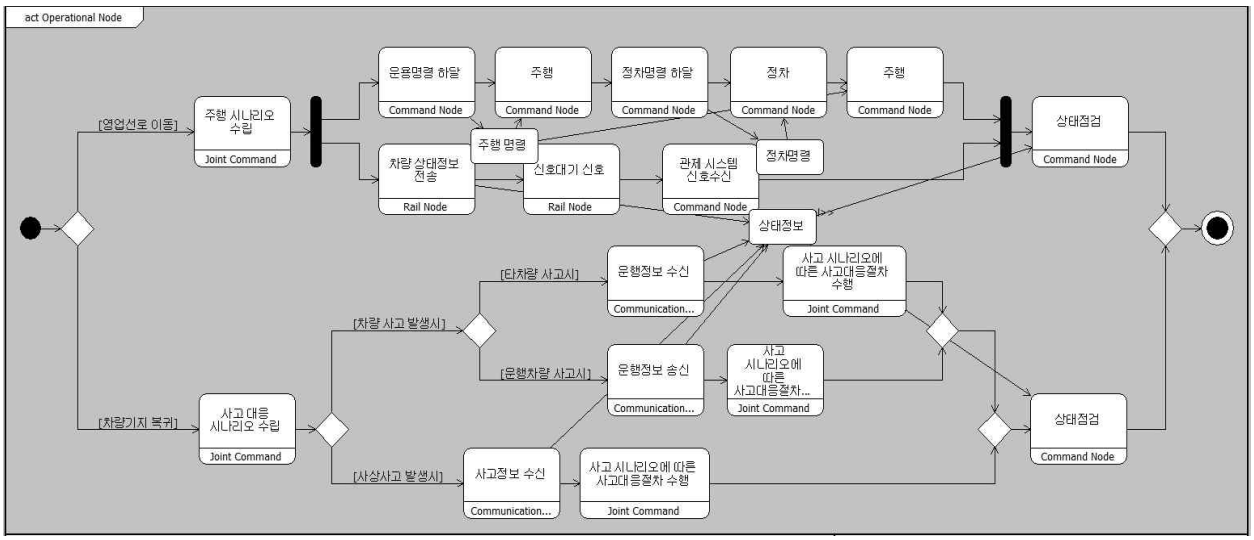
SysML은 서두에 언급한 것처럼, 표준 언어로서의 기능과 설계단계에서 분석, 검증, 확인을 수행하는데 있어서 실제 시제품을 만들기 전에 모델을 통해서 수행 가능하다는 점에서 개발단계에서 상당한 비용과 기간을 줄일 수 있다.

이러한, 장점을 근거로 미국의 경우, 군사, 우주항공, 철도, 자동차 등의 다양한 분야에서 폭넓게 이용되어 지고있다.

<Table 1>을 통해서, SysML의 특성을 분석·정리 하였으며, <Table 2>를 통해서, 일반적 설계관점과, 안전관점에서 분석·정리 하였다. 특히, <Table 2>를 통해, SysML을 개념설계 단계에서 분석 가능한 안전 활동을 기준으로 안전관점에서 분석 실시하였다. 서두에 언급한대로, SysML은 UML의 확장된 개념으로서 <Table 2>를 통해 식별할 수 있듯이, 기존 UML 기준으로 상응하는 다이어그램이나, 확장(Extension), 변경(Modified), 변경 없음(Unchanged)으로 표현하여 SysML과 상응 또는 변경사항에 대해인지 할 수 있도록 구분 하였다.

SysML은 다음과 같은 특징을 지니고 있다.

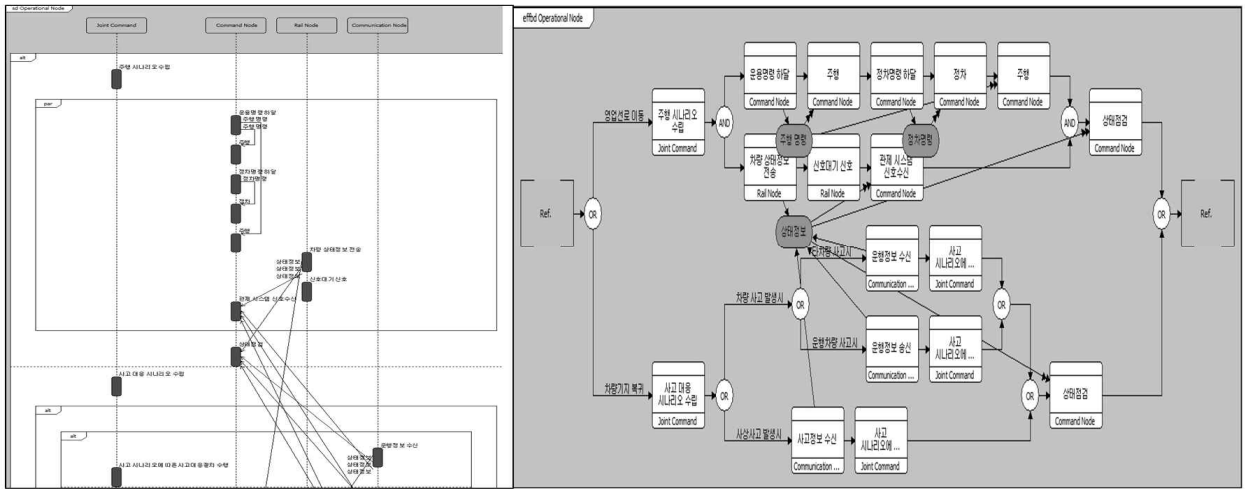
1. 표준언어(정보공유 및 동일한 이해 가능)
2. 그래픽 모델링 언어(시각적 정보전달 및 이해 가능)
3. 추적성(설계 변경 및 문제점, 영향도 분석 가능)
4. 콤팩트한 언어(이해와 공통화시 용이함)



<Figure 10> Activity diagram of the high-speed train

<Table 2> SysML diagrams analysis table a according to the view of the design and safety.

Design View	SysML Diagram	UML Diagram	Safety View
시스템이 지니고 있는 물리적 관점에서 체계의 구성에 대해 분석가능하다. 따라서, 시스템의 상위 수준에서 체계의 서브 구성에 대해 분석 가능한 정보를 제공한다. 식별된 기능을 컴포넌트에 할당하는 과정에서 이용가능.	Block Definition Diagram(BDD)	Class Diagram	설계단계에서 식별된 상위수준의 물리적 구성품을 나타내고 그에 따라 시스템을 구성하는 물리적 구성품의 기능을 식별하는데 정보제공. 식별된 기능 계층도를 바탕으로 기능요구사항과 기능 안전요구사항 생성 가능. 따라서, 최상위 수준의 위험원 분석 활동인 SHA를 수행하는데 있어서 활용 가능.
시스템 최상위 수준이 아닌 그 이하의 서브-시스템을 포함한 시스템의 컴포넌트 수준에서 시스템의 물리적 구성품 설계를 하는데 활용한다. 하부 시스템 체계를 구성하는 물리적 구성품을 표현하는데 활용가능.	Internal Block Diagram(IBD)	Composite structure Diagram	서브-시스템을 포함한 컴포넌트 수준에서 이행되어야 할 기능으로부터 식별된 기능요구사항 식별 및 생성에 활용. 따라서, SSHA, FTA를 수행에 필요한 서브-시스템 수준의 안전요구사항 정보 제공 및 분석적 기법을 제공한다.
시스템 성능요구사항을 표현하는데 있어서 PMD를 활용함으로써, 시스템이 지녀야할 요구사항과 시스템 설계 검증단계에서 수행 가능한 검증지표를 제공.	Parametric Diagram(PMD)	Extension	시스템 기능이 지녀야할 설계 성능요구사항으로부터 파생 가능한 기능안전 요구사항이 식별 가능하므로 시스템 안전성을 확보하는데 있어서 정량적 제약조건을 PMD을 통해서 제공 가능함.
동질의 속성 모델 요소 간 그룹화 하는데 활용 가능한 다이어그램으로서, 기능분석 수행과 컴포넌트 식별 수행을 통해 획득된 결과물을 바탕으로 동질의 모델을 그룹화 가능	Package Diagram(PKD)	Unchanged	시스템의 물리적 구성 등 기능에 관한 추상적 개념들을 모은 하나의 그룹을 패키지라고 한다. 본 다이어그램을 통해, 상속 또는 양방향 의존관계를 명시할 수 있다. 따라서, 시스템 안전 활동을 계획(SSPP)하고 상위수준의 물리적 구성 또는 기능으로부터 수행 가능한 SHA, SSHA를 수행하는데 상당한 정보제공.
설계 대상 시스템의 운용개념을 통해 시스템이 수행해야하는 동작에 대한 정보를 제공함으로써 작업이나 처리가 어떤 순서로 진행되는지, 어떠한 조건에서 수행되는가에 대해서 거동의 정보 분석이 가능하다. 따라서, 기능요구사항을 생성하는데 중요한 정보를 제공한다.	Activity Diagram(AD)	Slightly Modified	본 다이어그램을 통해, Activity를 처리하는 동안 두 개 이상의 클레스 객체들 간 제어 흐름을 보여준다. 따라서, 개별적 컴포넌트가 지니고 있는 기능 흐름 및 다른 컴포넌트의 기능 흐름에 따른 상호 연동성 식별이 가능함에 따라, 컴포넌트 수준에서 안전과 관련한 인터페이스 요구사항 생성이 가능. SSHA, FMEA 수행에 활용 하는데 효과적 이다.
설계대상 모델의 실시간 연속적 흐름을 제공한다. 또한, 시퀀스 다이어그램을 통해서 모델간의 상호 입·출력 산출물의 상호 호환성을 식별 가능하기 때문에 시스템 하부 체계의 기능 인터페이스 설계에 활용 가능하다.	Sequence Diagram(SD)	Unchanged	시스템을 구성하는 하위 구성 컴포넌트별 지니고 있는 기능의 흐름 정보를 제공 할 수 있다. 개별 컴포넌트의 목적을 달성하기 위한 기능 흐름의 정보를 제공. 기능의 흐름으로부터 기능 요구사항 및 기능안전 요구사항을 생성 가능하다.
시스템 상태 모드의 변화 추이의 정보를 제공함으로써 설계자가 고려해야할 정보를 제공한다.	State Chart(SC)	Unchanged	기능중심의 안전 활동을 보다 강화할 수 있는 방안으로 상태 전이 차트를 바탕으로 수행가능. 따라서, Activity와 Sequence 다이어그램을 통해서, 상태의 변화에 따라 시스템 기능분석 가능함에 따라, 기능요구사항 생성 및 검증을 수행하는데 있어서 활용가능
상위수준에서 시스템 인터페이스 및 기능 식별 정보 제공. 상위수준의 시스템 운용자 식별 가능.	Usecase Diagram(UCD)	Unchanged	기능관점의 안전성을 추구하기 위해서 상위수준의 기능 및 사용자 인터페이스로부터 발생 가능한 정보를 제공하여 기능요구사항 생성 근거제공. 최상위 기능을 식별하여 시스템의 내부의 하부 기능을 분화하는데 정보를 제공하여 기능안전성 확보에 활용가능. 초기 시스템 안전 계획을 수립 및 PHL, PHA을 수행하는데 있어서 필요한 정보 제공한다.
설계단계의 상위 운용개념으로부터 시스템 요구사항-하부 컴포넌트 요구사항까지의 요구사항 분화의 근거 및 변경 및 영향에 관한 정보를 제공 가능하다.	Requirements Diagram(RD)	Extension	설계요구사항-시스템 안전요구사항-안전 기능 요구사항 간 영향도 분석 및 추적성 정보 제공. 시스템 안전 기능 검증 및 확인을 수행하는데 있어서 근거의 문장을 제공한다. 따라서, 시스템, 서브-시스템 수준에서 기능 정보를 제공하기 때문에 PHL, PHA, SHA 필요로 하는 정보를 제공한다.



<Figure 11> Sequence Diagram(left) and Enhanced Function Flow Diagram(right)

4.2 SysML 기반 구축된 통합 프로세스 모델의 검증

<Figure 8>에서 제시되는 것처럼, SysML 기반 구축된 통합 프로세스 모델에 관한 검증과정을 수행하기 위해서, 시스템공학 전산지원 도구(Vitech CORE)를 활용하여 통합 모델의 논리적 오류 및 흐름 등에 대한 시간선 분석을 통해 검증 과정을 수행하였다. 따라서, 이러한 결과를 바탕으로 구축된 프로세스 모델에 대해 수정과정의 반복을 통해, 최적화된 설계 프레임을 갖출 수 있었다.

4.3 사례연구

시스템의 설계단계에서 안전성 확보를 위한 방안중 하나로 초기 개념설계 단계에 안전성 평가를 반영한 통합 프로세스 모델을 구축하였다. 따라서, 시스템 설계 프로세스를 기준으로 초기 이해당사자 요구사항으로부터 기능요구사항 및 기능안전 요구사항이 생성될 수 있도록 <Figure 8>에서 제시하는 RD를 통한 요구사항 생성 및 관리가 필요하다. RD를 통해서, 설계 요구사항으로부터 기능안전 요구사항으로 까지의 추적성을 활용해 변경에 따른 영향도 분석이 가능해 질 수 있다. 특히, UCD를 통해, 상위 수준의 시스템 사용자 및 인터페이스, 시스템의 상위 기능 식별이 가능하다. 따라서 이러한, 데이터를 근거로, BDD와 PKD를 통해서, 시스템 기능의 계층화를 수행 할 수 있다. BDD를 통해 상위 수준의 기능과 식별된 물리적 구성품을 바탕으로 안전활동에서 상위 수준이 PHL, PHA, SHA를 수행 가능 하도록 한다. 이러한 상위 수준의 기능 데이터는 IBD를 통해서 보다, 계층 수준을 낮춰 보다 상세한 내부 물리적 구성품을 표현 가능하다. 따라서, 보다 하위 수준의 기능과 물리적 구성품을 나타낼 뿐만 아니라, 기능요구사항과 관련한 보다 하위 수준의 요구사항에 관해 추출할 수 있는 근거를 IBD를 통해 추출 가능하다. 시스템의 설계단계에서 기능을 식별하고 관련한 요구사항을 정의 하기 위해서는 SD와 AD를 통해서 수행해야한다. SD와 AD를 통해, UCD 보다 세부 수준의 시스템 구성품의 거동을 분석 가능해진다. 오늘날 시스템 안전 추구 활동이 기능의 안전성으로부터 추구한다는 점에서 SD와 AD는 매우 밀접한 연관성을 지니고 있다.

SD와 AD를 보완하는 기법중 하나로 SC 활용을 제안한다. 상태의 변화에 따른 기능을 분석 가능하다는 점에서 보다 다른 시각에서 거동 분석이 가능해 진다. 기능 분석 단계를 거치면, 식별된 기능은 컴포넌트로 할당하는 단계를 거치게 된다. 위에서 언급한데로, 운용개념과 UCD를 통해 식별된 상위 물리적 시스템을 BBD와 PKD로 식별되었다. 또한, 이렇게 식별된 물리적 구성품은 IBD를 통해 보다 세분화 된다. 위에서 생성된 기능 요구사항을 과연 어떠한 물리적 구성품이 그 기능을 구현할지에 대한 할당을 하게 된다. 또한, 기능이 컴포넌트에 할당 되었다는 것은 해당 기능요구사항이 지녀야할 기능 안전 요구사항을 생성할 수 있고, 기능 오류시 어떠한 컴포넌트에 영향이 미치는지 영향도 분석이 가능해 진다. 따라서, SSHA와 그 이하 컴포넌트 수준의 안전 분석을 수행하는데 필요한 근거를 제공하게 된다.

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

5. 결론 및 요약

본 연구에서는 시스템의 설계 프로세스와 안전 활동 프로세스와의 통합을 시도하였다. SysML이라는 공통 언어를 사용함으로써 서로 다른 분야의 엔지니어들이 연구의 결과에 대하여 공통의 인식을 갖게 할 뿐만 아니라 결과적으로 설계와 안전 활동에 활용할 수 있는 방안을 제시하였다.

따라서, 본 논문에서는 대형복합 안전중시 시스템의 안전성 강화 방안으로 기존에 상세설계단계에서 집중적으로 시행 해왔던 안전 활동을 개념설계에서 이행 가능한 하나의 통합 프로세스 모델을 제시하여 개발단계의 기간과 비용 측면에서 상당히 줄 일 수 있다. 제시된 통합 프로세스 모델은 SysML이 지원하는 개별적 다이어그램으로부터 개별 고유의 특성을 통해 설계활동과 안전 활동에 대한 실현을 대체 구현 가능한 방법을 제시하여 동일한 이해아래 커뮤니케이션이 가능하도록 제시하였다. 또한, 안전성 확보 방안이 보다 초기에 적용됨에 따라, 설계 안전성 측면에서도 상당한 기여를 하였다고 판단된다. 후속 연구 활동 또한 활발히 진행되었으며 하며, 추후 연구에서는 연구범위를 확장 시키는 연구가 필요 할 것이다.

6. 참 고 문 헌

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

[2] K. Thramboulidis and S. Scholz, "Integrating the 3+1 SysML view model with safety engineering," Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on, pp. 1-8, 13-16 Sept. 2010.

[3] S. Friedenthal, A. Moore, and R. Steiner, A practical guide to SysML: the systems modeling language. Access Online via Elsevier, 2011.

[4] D. Torsten and A. H. Jorg, "How to “Survive” a safety case according to ISO 26262," in Proc. Computer Safety, Reliability, and Security, 2010, pp. 97-111.

[5] J. Y. P and Y. W. P, "Model-based Concurrent Systems Design for Safety," Concurrent Engineering, vol. 12, no. 4, pp. 287-294, December 1, (2004)

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

[7] S. Sierla, I. Tumer, N. Papakonstantinou, K. Koskinen, and D. Jensen, "Early integration of safety to the mechatronic system design process by the functional failure identificat ion and propagation framework," Mechatroni cs, vol. 22, no. 2, pp. 137-151, 2012.

[8] Processes for Engineering a System, EIA STANDARD 632, (1994).

[9] MIL-STD-882D Standard Practice for Syste m Safety Program Requirement, 2000.

[10] A. Kossiakoff, W. N. Sweet, S. Seymour, a nd S. M. Biemer, Systems Engineering Principles and Practice. vol. 83: Wiley, (2011)

[11] 체계공학(SE) 표준지침(안), 방위사업청, (2010)

저 자 소 개

김 영 민

현 아주대학교 시스템공학과 박사과정. 관심분야는 시스템 안전설계, 요구사항 관리, 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