안전중시 시스템을 위한 체계적인 설계 프로세스에 관한 연구

윤 재 한* · 이 재 천*
*아주대학교 시스템공학과

A Process Model for the Systematic Development of Safety-Critical Systems

Jae-Han Yoon* · Jae-Chon Lee*
*Department of Systems Engineering, Ajou University

Abstract

It is becoming more and more important to develop safety-critical systems with special attention. Examples of the safety-critical systems include the mass transportation systems such as high speed trains, airplanes, ships and so forth. Safety critical issues can also exist in the development of atomic power plants that are attracting a great deal of attention recently as oil prices are sky-rocketing. Note that the safety-critical systems are in general large-scale and very complex for which case the effects of adopting the systems engineering (SE) approach has been quite phenomenal. Furthermore, safety-critical requirements should necessarily be realized in the design phase and be effectively maintained thereafter. In light of these comments, we have considered our approach to developing safety-critical systems to be based on the method combining the systems engineering and safety management processes. To do so, we have developed a design environment by constructing a whole life cycle model in two steps. In the first step, the integrated process model was developed by integrating the SE (ISO/IEC 15288) and systems safety (e.g., hazard analysis) activities and implemented in a computer-aided SE tool environment. The model was represented by three hierarchical levels: the life-cycle level, the process level, and the activity level. As a result, one can see from the model when and how the required SE and safety processes have to be carried out concurrently and iterately. Finally, the design environment was verified by the computer simulation.

Keywords : Safety Requirements, Systems Engineering Process, Design Environment, Safety-Critical Systems, Hazard Analysis Techniques

1. 서 론

오늘날 많은 시스템 개발에서 시스템의 안전이 전체 시스템 수명주기 동안 고수준으로 유지되도록 요구되고 있다. 이에 반해, 시스템들은 점차 그 규모가 커지고 복잡성이 증대하여, 시스템의 성공뿐 아니라 시스템의 안전을 목표한 수준을 실현하는데 다양한 문제점들이 제기되고 있다. 시스템 안전의 근본적인 목적은 시스템 위험원을 식별하고, 제거하거나 통제하고, 문서화하는 것이다.[1] 시스템 안전 공학은 시스템공학의 한 구성요소로 진술된다. 그리고 시스템공학은 위험원을 적시에 식별하고 시스템에 내재된 위험원을 방지하거나

† 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2008-313-D01245)
† 교신저자: 이재천, 경기도 수원시 영통구 원천동 산5번지, 아주대학교 서관 309호
Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
2009년 7월 10일 접수; 2009년 8월 28일 수정본 접수; 2009년 8월 28일 게재확정

통제하기 위해 필요한 활동들을 착수시키기 위한 과학적이고 공학적인 원리의 응용을 포함한다.[1]

안전 중시 시스템들이 더욱 복잡해지면서, 성공적인 시스템 개발을 실현하도록 다학제적 수단을 제공하는 시스템공학 접근법이 안전 중시 시스템 개발에 확산되고 있다.[2]

안전과 관련한 모든 활동은 시스템 설계 개념 초기부터 상세 설계, 시험, 그리고 시스템 폐기에 이르기까지 전체 시스템 수명주기 전반에서 수행되어야 한다.[1]

Federal Aviation Administration (FAA) 는 Acquisition Management System (AMS) 의 수명주기를 정의하고, 수명주기 전반에 걸친 안전 위험도 관리 방침을 정의하였다.[3][4] 안전 위험도 관리 방침은 각 단계마다 수행해야할 안전성 평가 활동과 작성해야할 계획서 등을 나타내며, 각 수명주기 단계별로 수행해야할 적절한 위험원 분석 기법들을 기술하고 있다. 이러한 지침에 따라, FAA는 시스템 위험도 관리 결과를 시스템의 설계에 반영토록 하고 있다.[4]

위험원 분석을 통해 얻은 결과는 시스템 설계에 반영되어야 한다.[5] 그리고 시스템 안전 활동은 실제 시스템 개발과 함께 수행되어야 한다.[1] 이러한 맥락에 따라, 시스템공학과 시스템 안전 활동의 통합 수행에 대한 연구가 있었다. 시스템공학, 시스템 안전 분석, 그리고 인간 요소를 기반으로 한 통합 시스템 설계 방법을 개발한 연구가 참고문헌 [6]에 발표되어 있다. 또한 참고문헌 [7]에는 설계와 안전 분석을 통합하고, 소프트웨어 아키텍처의 위험원 분석과 하드웨어 안전 분석을 조화시키고 있다. 참고문헌 [8]에는 개량된 기능 위험원 분석 평가 방법과 유즈케이스 방법을 통합하고 있다. 이러한 연구들과 본 연구의 차이점은 1) 위험원 분석을 시스템 수명주기와 계층구조을 중심으로 상세화하였으며 2) 시스템 설계가 시스템공학 프로세스들의 반복적인 수행을 통해 이루어지도록 반영하였으며 3) 위험원 분석을 위한 프로세스들이 시스템 요구사항과 시스템 설계의 기능적 및 물리적 요소들과 동기화되도록 하였다.

본 연구는 시스템공학 중심의 안전 설계 방안을 제시하고, 그에 따른 개발 환경 구축 방안을 제시하고자 한다. 시스템공학에서는 개발 환경을 정의하기 위해 프로세스, 방법, 도구, 환경 요소를 정의한다.[2] 이에 따라, 본 연구에서는 안전 설계를 위한 시스템공학과 안전 분야의 통합 프로세스를 설계하였다. 방법적인 측면에서는 안전 확보를 위해 활용할 위험원 분석 기법들을 정의하였다. 도구와 환경은 특정 개발 환경에 종속되지 않기 위해 제한하지 않았다. 하지만 설계 데이터들의 추적성 및 일관성을 확보하기 위해, 설계 데이터 관리를 위한 데이터 모델을 통합 프로세스를 기반으로 설계하였다. 이는 설계 데이터를 만들어내는 분석 및 개발 도구나 설계 데이터를 관리하는 데이터베이스 도구들에 독립적이다.

본 논문은 다음과 같이 구성되어 있다. 2장은 본 연구의 문제에 대한 기본 개념과 배경을 기술한다. 3장은 개발 환경 구축을 위한 프로세스 모델링 방안을 기술한다. 4장은 통합 프로세스 모델에 대한 상세한 설명을 제공한다. 5장은 모델 검증을 기술한다. 마지막으로 여섯 번째 장은 결론을 기술한다.

2. 시스템공학 및 시스템 안전

2.1 시스템 수명주기와 위험원 분석

시스템 안전은 전 시스템 수명주기 동안 보장되어야 한다고 앞에 언급하였다. <그림 1>의 수명주기 모델에 따라, 각 수명주기 단계마다 수행해야하는 적절한 위험원 분석 활동들은 참고문헌 [1]에 기술되어 있다. 그리고 이를 <표 1>과 같이 정리하였다.

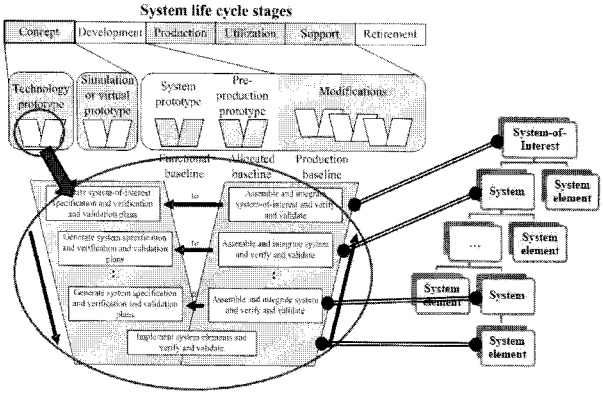
<table>
<tr><td rowspan="2">Concept Definition</td><td colspan="3">Engineering Development</td><td rowspan="2">Production</td><td rowspan="2">Operation</td><td rowspan="2">Disposal</td></tr>
<tr><td>PD</td><td>DD</td><td>Test</td></tr>
</table>

<그림 1> 안전 중시 시스템 개발을 위한 수명주기 모델 예 [1]

<표 1> 수명주기 모델 예를 기반으로 수행되는 각 단계별 위험원 분석 기법 [1]

위험원 분석 기법	수명주기 단계
Preliminary Hazard List Analysis (PHL)	CD-PD
Preliminary Hazard Analysis (PHA)	CD-PD
Sub System Hazard Analysis (SSHA)	DD
System Hazard Analysis (SHA)	PD-DD-T
Functional Hazard Analysis (FHA or FuHA)	CD-PD-DD
HAZard and OPerability analysis (HAZOP)	PD-DD
Failure Mode, Effects and Analysis (FMEA or FMECA)	PD-DD

CD: Concept Definition, T: Test



<그림 2> ISO/IEC 15288:2002에서의 수명주기, 계층구조, Vee 모델 [9],[12]

2.2 시스템공학을 통한 시스템 설계 개념

시스템 안전 확보를 위해 시스템공학적 접근법을 도입하기 위해, 본 연구에서는 여러 시스템공학 개념들 중에서도 국제 표준인 ISO/IEC 15288:2002 [9]를 활용하였다. 이는 15288이 국제 표준이자 전체 시스템 수명주기를 고려한 표준이기 때문이며, 다른 시스템공학 표준들과도 조화를 이루도록 개정 활동이 이루어지고 있기 때문이다. 예를 들어, 최근 개정된 IEEE 1220-2004 [10]나 EIA-632a [11]가 그것이다. 그리고 15288의 올바른 활용을 위하여, 15288의 활용에 대한 지침을 제공하는 ISO/IEC TR 19760:2003 [12]을 참고하였다.

15288은 <그림 2>의 상부와 같이 6단계로 시스템 수명주기를 기술하고 있다. 그리고 19760에서는 각 단계마다 <그림 2>의 하위 Vee 모델을 기반으로 시스템 개발 활동을 권하고 있다. 그리고 Vee 모델 기반의 개발 활동은 <그림 2>의 우측의 시스템 계층구조에 맞춰서 시스템을 각 계층별로 세분화시킨다. 그리고 각 시스템의 계층 별로 Vee 모델에 맞춰 반복적/점진적 설계를 수행한다.

2.3 시스템공학과 시스템 안전의 연관성

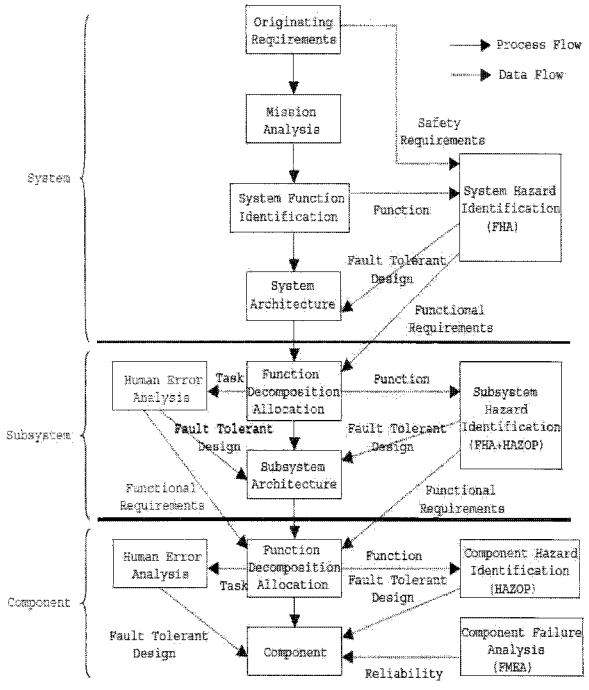
앞에서 시스템공학과 시스템 안전의 동시공학적인 수행에 대한 몇몇 연구 결과들을 언급하였다. 그들 중, 참고문헌 [6]의 연구 내용이 우리의 연과 내용과 가장 유사하다. 참고문헌 [6]는 시스템공학 프로세스를 요구사항 분석, 기능 분석, 합성, 그리고 시스템 분석 및 최적화로 정의하고 각 시스템 수준에 따른 위험원 분석 기법을 정의하였다. <그림 3>와 같이, 기본적으로 시스템 설계 프로세스는 3 수준의 계층구조에 따라 수행되고 각 설계 프로세스와 연관된 위험원 분석 기법을 나타내었다. 그리고 제안한 설계 방법론에 따라, CORE®[13]를 통해 설계 환경을 구축한 예를 포함하고 있다. <그림 3>에서 보듯이, 참고문헌 [6]의 연구는 시스템공학 프로세스들이 위험원 분석 기법들에 의해 추가/개선되었다고 볼 수 있으며, 본 연구는 이를 기반으로 시스템공학과 시스템 안전 활동을 통합한 개발 환경을 제시한다.

2.4 시스템공학과 시스템 안전의 통합

<그림 3>의 모델에는 기능 중심의 위험원 분석 활동에만 초점이 맞춰져 있으며, 순차적인 개발 양상을 보인다. 하지만, 본 연구에서는 ISO/IEC 15288을 기반으로 시스템 수명주기 전반을 고려하여 위험원 분석 활동을 정의하고, 반복적/점진적 개발 양상을 보인다.

이는 시스템공학 활동과 안전 활동을 잘 융합하고, 시스템의 안전을 더욱 높이기 위함이다.

두 분야의 활동을 통합하기 위해서는, 두 분야의 활동 간의 인터페이스 정의가 중요하다. 인터페이스란 두 분야의 활동들이 어떠한 산출물들을 어느 시점에 주거나 받는지 정의한 것이다. 본 논문은 안전 요구사항 반영을 위해, 시스템 수명주기와 시스템의 계층구조에 따라 어떠한 위험원 분석 결과를 시스템 설계에 반영해야 하는지 정의하였다.



<그림 3> 안전을 위한 동시공학적 시스템 설계 프로세스에 대한 접근 사례 [6]

통합 개발 환경은 결과적으로 시스템공학과의 연계를 통해 시스템 안전 향상과 시스템의 생산성을 향상시킬 것이다. 여기서 통합은 시스템공학과 위험원 분석 활동의 단순한 합으로 기술되어 있지 않다.

3. 통합 설계 환경을 위한 모델 개발

3.1 설계 프로세스 및 데이터 관리 모델

통합 개발 환경을 구축하기 위해, 프로세스와 방법을 우선적으로 정의할 필요가 있었다. 이를 효율적으로 정의하고 표현하고 관리하기 위해, 프로세스와 방법을 나타내는 모델을 개발하였다. 그리고 모델 개발에 필요한 모델링 도구의 사용이 필요하였다. 본 연구에서는 프로세스의 흐름과 각 프로세스에서 사용되는 여러 방법들, 그리고 프로세스 간의 연관관계 등을 표현하기 위해, 향상된 기능 흐름 블록도 (EFFBD)를 선정하였다.

EFFBD는 기능 흐름 블록도 (FFBD) [14]의 확장판으로 입출력 데이터를 추가적으로 표현할 수 있다. 그리고 EFFBD를 효율적으로 활용하기 위해, CORE®라는 도구를 활용하였다.

프로세스와 방법에 따라 개발을 지원하게 될 도구에 대해서는, 특정 도구에 종속되지 않고 안전 요구사항을 충실히 반영할 수 있도록 설계 데이터 관리 모델을 개발하였다. 이는 개발 시 활용되는 각 방법들을 지원하는 도구들로부터 발생하는 설계 데이터들이 서로 어떤 연관 관계를 가지는지, 즉 어떤 추적성 관계가 있는지를 표현한다. 이로 인해, 안전 요구사항들이 어떤 설계에 어떤 관계가 있는지를 표현하고, 이러한 데이터들 간의 연관성을 고려하여 일관성을 유지할 수 있도록 지침을 제공한다. 설계 데이터 관리 모델은 데이터들 간의 일관성 및 추적성을 관리하기 위한 모델로서, 데이터들의 DB를 구성하여 관리하도록 DB 스키마 [15] 형태로 개발하였다. 그리고 스키마는 일반적으로 널리 사용되는 ER 도면 [16] 형식으로 표현하였다.

3.2 모델링 절차 요약

모델을 개발하기 위해, 우리는 다음과 같은 절차를 수립하였다. 각각의 활동을 통한 결과들이 모델에 반영되었다.

1) 시스템 수명주기를 여러 단계로 정의한다.
2) 각 수명주기 단계별로 적절한 위험원 분석 기법을 정의한다.
3) 시스템 계층구조에 따라 각 수명주기 단계별로 시스템 수준과 Vee 모델을 정의한다.
4) Vee 모델을 기반으로 시스템공학 프로세스들을 정의한다.
5) 각 수명주기 단계별로 수행되는 위험원 분석 기법들과 연계되는 시스템공학 프로세스를 정의한다.
6) 시스템공학과 시스템 안전 프로세스 사이의 인터페이스를 식별한다.
7) 인터페이스를 기반으로 서로 연관된 설계 데이터를 정의한다.

3.3 설계 프로세스 모델의 구조

모델은 세 수준으로 설계되어 있다. 첫 번째 수준은 시스템 수명주기 수준, 두 번째 수준은 프로세스 수준, 그리고 세 번째 수준은 활동 수준이다. 두 번째 수준에서 시스템공학과 시스템 안전 프로세스 사이의 인터페이스가 표현되며, 이에 따라 두 분야의 프로세스들 사이의 교환 데이터가 표현되어 있다. 실제 해당 데이터가 어떠한 활동으로부터 발생하는지는 세 번째 수준에서 나타난다.

세 수준으로 설계된 모델은 CORE®의 EFFBD 모델링 기능으로 구축되어 있다. 수명주기의 각 단계, 프로세스들, 활동들은 기능 블록으로 나타내어져 있고, 교환 데이터들은 데이터 블록으로 나타내어져 있다. 각 기능 블록들은 다음 수준의 EFFBD 모델로 분해가 되는데, 예를 들어 첫 번째 수준 모델의 수명주기 각 단계는 해당 단계의 프로세스들을 표현한 프로세스 모델로 분해된다. 그리고 프로세스 모델에서 기능 블록으로 표현된 프로세스는 해당 프로세스의 활동들을 나타내고 있는 활동 모델로 분해된다. 각 수준에 따른 모델의 연관성을 관리하기 위해 CORE®의 추적성 관리 기능은 매우 유용하였다.

4. 통합 설계 환경의 구축

4.1 모델링 범위

ISO/IEC 15288:2002의 수명주기 단계 중, 본 연구에서는 시스템 개발과 직접 관련된 단계에 중점을 두었다. 예를 들어, 개념 단계와 개발 단계이다. 그리고 전체 25개의 15288 프로세스들 중 기술 프로세스 그룹에 속하는 11개의 프로세스 중 운영, 유지보수, 그리고 폐기 프로세스들은 배재한 나머지 8개 프로세스에 집중한다.

위험원 분석 프로세스의 경우에는, 복잡도를 줄이고

원래 취지를 유지하기 위해, 참고자료 [1]와 [6]의 연구를 기반으로 중요한 위험원 분석 기법들을 선정하였으며, 이는 <표 2>와 같다.

4.2 설계 프로세스 모델

프로세스 모델의 최상위는 수명주기 단계들로 구성되어 있으며, 수명주기 관점 모델이라 부를 수 있다.

수명주기 단계는 stage와 phase로 구성되고, stage가 phase로 분해되면서 수명주기 모델은 확장되어 있다.

이는 수명주기가 여러 단계들로 구성되어 있음을 의미한다. 각 수명주기 단계에는 Vee 모델이 할당되어 있는데, 프로세스 관점 모델은 Vee 모델을 나타낸다.

Vee 모델을 좌측부, 중앙부, 우측부로 나누어서 첫 번째 프로세스 관점 모델로 표현하였다. 그리고 두 번째 프로세스 관점 모델에서 Vee 모델의 좌측부에는 이해당사자 요구사항 정의, 요구사항 분석, 아키텍처 설계 프로세스를 나타내었고, Vee 모델의 중앙부에는 구현 프로세스를 나타내었으며, Vee 모델의 우측부에는 통합, 검증, 이전, 확인 프로세스를 나타내었다. 마지막으로 활동 모델은 프로세스 관점 모델이 분해되어서 각 프로세스 별 활동을 나타내도록 구성되어 있다. <그림 4>에서 구성된 모델과 계층구조를 확인할 수 있다.

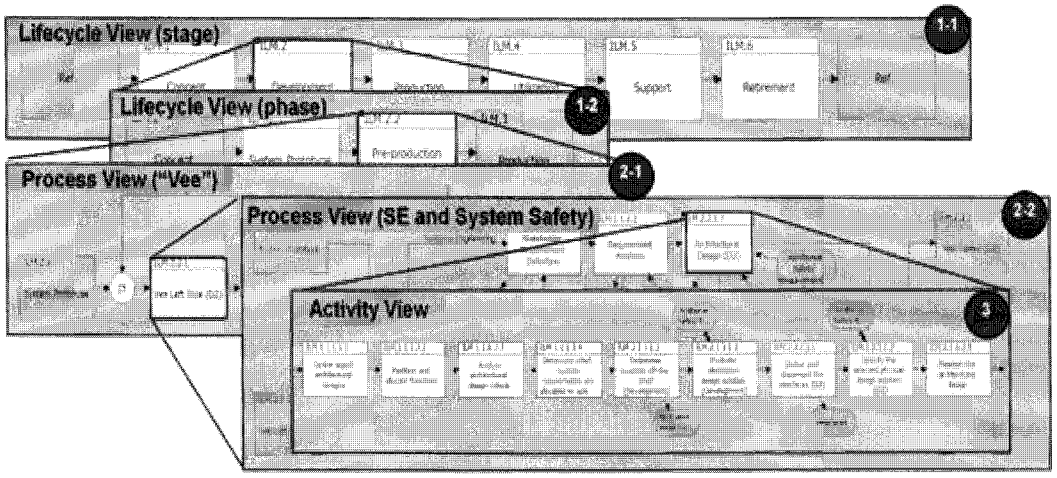
4.3 설계 시 위험원 분석의 통합 수행을 통한 안전 요구사항 반영

<표 2>는 ISO/IEC 15288:2002의 시스템공학 프로세스와 시스템 안전 프로세스 중 위험원 분석 기법을 수명주기 각 단계마다 비교한 것이다. <그림 1>과 참고문헌 [1]에서 제시한 수명주기를 비교하여 <표 3>과 같이 위험원 분석 기법들을 정리하고, 이를 <그림 1>의 수명주기에 맞춰 시스템공학 프로세스와 위험원 분석 기법을 연관지었다. 참고문헌 [6]에서 사용된 위험원 분석 기법들이 <표 3>에도 반영되어 있음을 알 수 있다. 위험원 분석 기법의 수행 순서 또한 반영되어 있다. 반면, 시스템공학과 위험원 분석 기법 간의 인터페이스는 ISO/IEC 15288의 시스템공학 활동들에 대한 설명과 각 위험원 분석 기법이 발생하는 산출물의 성격을 분석하여 결정하였다.

몇 가지 위험원 분석 특징들을 간단하게 살펴보면, 우선 PHL은 <표 3>에 의거하여 CD에서 수행되므로, Concept 단계 초기에 수행한다. PHA는 <표 3>에 의거하여 CD와 PD에서 수행된다. Simulation or virual prototype 단계에서는 적합성 연구가 이루어지며, 적합한 시스템 개념을 정의하는 단계에서의 시스템 기술(description)은 예견된 위험도를 포함해야만 한다.[12],[17]

PHL은 risk 분석이 없으므로, PHA를 Simulation or virual prototype 단계에 수행해야 한다.[1] SSHA는 DD에서만 수행되므로 <표 3>에 의거하여 Pre-production prototype 단계에서만 이루어진다. SHA는 보통 SSHA가 사실상 완료되었을 때 개시한다.[1] 그러므로 SHA는 Pre-production prototype 단계에서만 이루어진다.

기능 위험원 분석 (FHA)는 단독으로 수행되지 않고 PHA나 SSHA와 같은 다른 위험원 분석들과 함께 수행된다.[1] 이해당사자 요구사항 정의 프로세스는 보건, 안전, 보안, 환경, 그리고 다른 이해당사자의 요구사항과 중요 품질에 관련된 기능들을 규정한다. 그러므로, 이해당사자 요구사항 정의 프로세스는 PHL, PHA, 그리고 SSHA와 함께 수행되어야 한다.



<그림 4> 개발된 설계 프로세스 모델의 계층구조

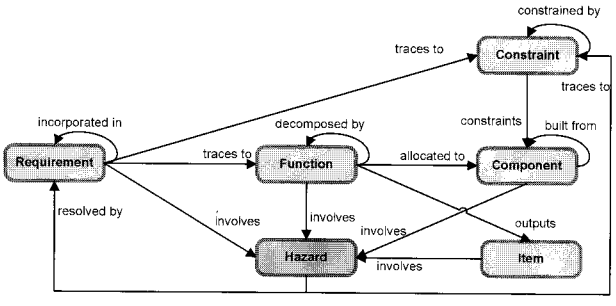
<표 2> 안전 요구사항 반영을 위한 시스템 설계 방안

SE Process	Hazard Analysis Technique			
	Concept Stage		Development Stage	
	Technology prototype	Simulation or virtual prototype	System prototype	Pre-prototype
Stakeholder Requirement Definition	- PHL	- PHA	- PHA	- SSHA
Requirements Analysis	- FHA	- FHA	- FHA	- HAZOP
Architectural Design			- HAZOP	- FMEA - SHA
Implementation				
Integration				
Verification				
Transition				
Validation				

<표 3> ISO/IEC 15288:2002의 수명주기에 맞춘 위험원 분석 기법

Concept Definition		Concept
Engineering Development	PD	System prototype
	DD	Pre-production prototype
	Test	Pre-production prototype
Development		
Production		Production
Operation		Utilization
		Support
Disposal		Retirement

SHA는 시스템 통합의 결과물을 기반으로 상세 위험원을 분석하는 활동이다.[1] 인터페이스 관련 위험원이 하위 시스템 인터페이스 정보를 기반으로 SSHA에서 예비 분석되고, 인터페이스 기술서를 기반으로 SHA에서 자세히 분석된다.[1] 그러므로 SHA는 아키텍처 설계 프로세스와 함께 수행한다.



<그림 5> 안전 요구사항 반영을 위한 설계 데이터 관리 모델

4.4 설계 데이터 관리 모델

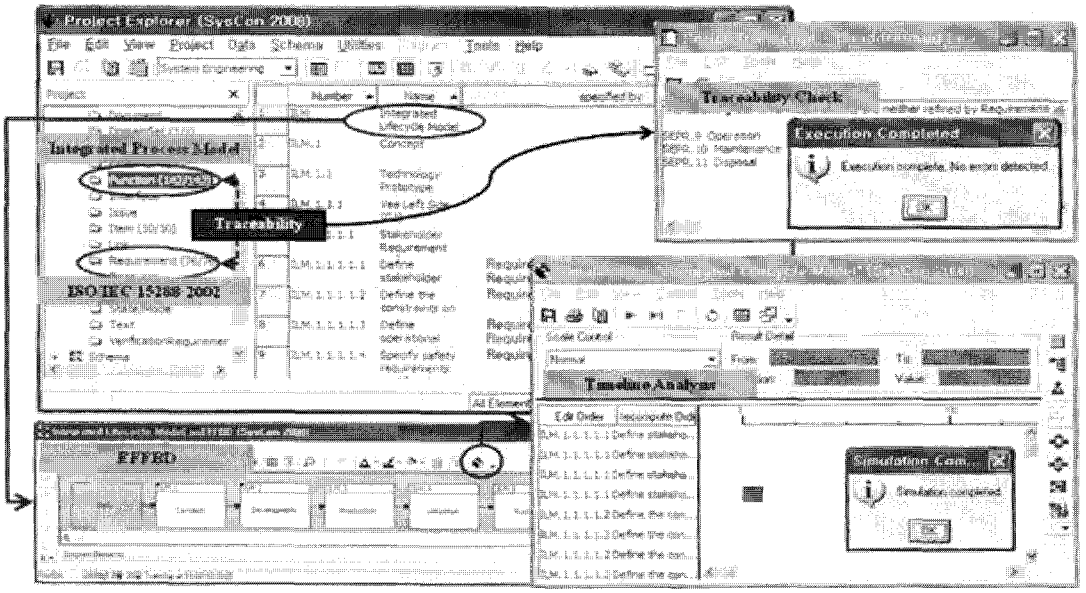
데이터베이스 스키마 (ER 도면 형식으로 표현)는 설계 프로세스 모델로부터 도출하였다. 참고문헌 [6]의 연구와 같이, CORE®에서 제공하는 기본 스키마를 바탕으로 "Hazard" (위험원)이라는 개체를 추가함으로써 스키마를 수정하였으며, 관계 설정의 경우는 위험원 분석 기법들의 추가 및 점진적/반복적 수행을 고려하여 개체간의 관계를 정의하였다. 개발된 스키마는 <그림 5>과 같으며, 다음 2가지 기준을 만족하도록 검토하였다.

- 스키마의 "객체"는 통합 프로세스 모델에서 데이터 블록으로 나타나는 설계 데이터들을 모두 포함.
- 스키마의 "관계"는 통합 프로세스 모델에서 하나의 기능 블록에 대한 입력 데이터 블록과 출력 데이터 블록간의 추적성을 모두 포함.

5. 통합 설계 환경에 대한 모델 검증

설계 프로세스 모델은 EFFBD로 설계하였으며, CORE®를 통해 구현되어 있다. 모델은 실행 가능한 모델로 구성되어 있으며, 시간선 분석을 통해서 시뮬레이션하였다. 시간선 분석을 통해, EFFBD 모델의 논리적인 오류를 검출하고, 시스템공학과 시스템 안전 사이의 동시공학적 수행 절차를 확인할 수 있었다. 그리고 모델은 이를 통해 지속적으로 개선하였다. 결과적으로 완성된 모델은 <그림 6>의 상단에서 확인할 수 있다.

다음으로 ISO/IEC 15288에 기술된 시스템공학 활동들이 모두 통합 프로세스 모델에 반영되었는지 검사하였다. 이를 위해, ISO/IEC 15288:2002의 시스템공학 활동과 연관된 활동 관점 모델의 기능 블록간에 추적성을 확보하였는지 분석하였다.



<그림 6> CORE®를 사용한 모델 실행 결과

이는 CORE®에서 제공하는 "Unaddressed Leaf-Level Requirements Query" 보고서 출력을 통해 수행하였다.

이는 모델에 반영되어 있지 않는 시스템공학 활동들을 정렬할 수 있다. 결과적으로, 모든 기술 프로세스들이 모델에 반영되어 있음을 확인하였다. 단, 운영, 유지보수, 그리고 폐기 프로세스들은 본 연구 범위에서 제외되어 있기에 <그림 6>과 같이 검출되어 있음을 확인할 수 있다.

마지막으로, ISO/IEC 15288:2002의 시스템공학 활동, 통합 프로세스 모델, 그리고 CORE®로 구성된 통합 프로세스 모델간의 추적성 검사를 수행하였다. <그림 6>과 같이 ISO/IEC 15288:2002의 시스템공학 프로세스들은 "Requirement"로, 모델의 기능 블록들은 "Function"으로, 그리고 모델의 데이터 블록들은 "Item"으로 CORE®에 기록하여 추적성을 확보하였다.

6. 결 론

본 연구는 ISO/IEC 15288:2002의 기술 프로세스와 시스템 안전을 위한 위험원 분석의 통합 수행 방안을 제시함으로써, 설계 시 안전 요구사항을 반영하기 위한 방안으로 통합 설계 환경을 구축하였다. 그리고 통합 설계 환경을 표현하기 위해 모델을 개발하였으며, 모델을 통해 시스템공학 활동과 위험원 분석 기법들의 통합 수행을 규정하였다. 그리고 어떠한 위험원 분석을 통해 안전 요구사항을 작성하여 설계에 반영하는지 나타내었다.

설계 환경을 나타내는 첫 번째 모델인 설계 프로세스 모델은 세 수준의 계층구조를 가지도록 설계되었으며, EFFBD를 통해 표현되어있다. 세 수준은 상위에서부터 각각 수명주기 관점, 프로세스 관점, 그리고 활동 관점으로 불린다. 그리고 모델의 두 번째 수준인 프로세스 관점에서 시스템공학과 시스템 안전 프로세스 사이의 인터페이스가 나타나있다. 설계 프로세스 모델을 기반으로 설계 데이터 관리 모델을 제시하였으며, 설계 프로세스에 따른 설계 활동과 산출물들의 관리를 위한 틀을 제시하였다.

설계 프로세스 모델은 CORE®을 통해 구현되어 있다. 개발된 모델을 검증하기 위해, 시간선 분석과 "Unaddressed Leaf-Level Requirements Query" 보고서 출력, 그리고 전체 추적성 검토를 수행하였다. 차후 변경된 시스템 개발 환경에 따라 설계 프로세스 모델 을 쉽게 변경하는데, 현재 확보한 추적성이 도움이 된다. 결과적으로, 본 연구에서 제시한 통합 개발 환경은 시스템공학과 시스템 안전에 대해 필요한 프로세스와 활동, 그리고 인터페이스를 규정하고 있다. 그리고 모든 프로세스와 활동들은 동시공학적으로 그리고 반복적으로 수행한다.

본 연구는 연구 범위에서 배제된 ISO/IEC 15288:2002의 다른 수명주기 단계들을 포함하여 전체 수명주기로 확장될 수 있다. 그리고 Vee 모델의 좌측부에 해당한 위험원 분석 기법들과 같이, Vee 모델의 우측부에 해당하는 통합, 합성, 그리고 검증과 확인 프로세스들과 관련한 시스템 안전 활동에 대한 연구가 필요하다.

7. 참 고 문 헌

[1] I. Clifton A. Ericson, Hazard Analysis Techniques for System Safety. Hoboken, New Jersey: John Wiley & Sons, Inc., 2005.

[2] N. M. James, Systems Engineering Guidebook: CRC Press, 1996.

[3] http://www.faa.gov/, Federal Aviation Administration, 2008.

[4] Safety Risk Management Guidance for System Acquisitions (SRMGSA), Federal Aviation Administration, 2007.

[5] N. Leveson, SafeWare : System Safety and Computers. Reading, Mass.: Addison-Wesley, 1995.

[6] J. Y. Park and Y. W. Park, "Model-based concurrent systems design for safety," Concurrent Engineering-Research and Applications, vol. 12, pp. 287-294, Dec 2004.

[7] Y. Papadopoulos, J. McDermid, R. Sasse, and G. Heiner, "Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure," Reliability Engineering and System Safety, vol. 71, pp. 229-247, 2001.

[8] J. Per, G. Christian, A. Anders, E. Ulrik, and T. Jan, "Hazard Analysis in Object Oriented Design of Dependable Systems," in Proceedings of the 2001 International Conference on Dependable Systems and Networks (formerly: FTCS): IEEE Computer Society, 2001.

[9] "Systems Engineering - System life cycle processes," in ISO/IEC 15288:2002(E): International Organization for Standardization, 2002.

[10] "IEEE Standard for Application and Management of the Systems Engineering Process," in IEEE Std 1220TM-2005: The Institute of Electrical and Electronics Engineers, Inc., 2005.

[11] "Processes for Engineering a System," in EIA-632a: The G-47 SE Committee of the Government Electronics and Information Technology Association (GEIA), 2005.

[12] "Systems Engineering - A guide for the application of ISO/IEC 15288 (System life cycle processes)," in ISO/IEC TR 19760: International Organization for Standardization, 2003.

[13] http://www.vitechcorp.com/, Vitech Corporation, 2008.

[14] B. S. Blanchard and W. J. Fabrycky, Systems Engineering and Analysis, 4 ed: Prentice Hall, 2005.

[15] A. Silberschatz, H. F. Korth, and S. Sudarshan, Database System Concepts, 5th ed. Boston: McGraw-Hill Higher Education, 2006.

[16] C. Peter Pin-Shan, "The entity-relationship model toward a unified view of data," ACM Trans. Database Syst., vol. 1, pp. 9-36, 1976.

[17] A. Kossiakoff and W. N. Sweet, Systems Engineering Principles and Practice. Hoboken, N.J.: Wiley-Interscience, 2003.

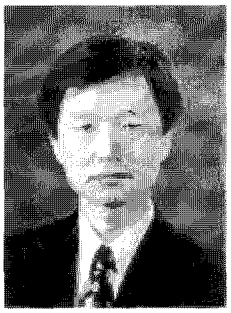
저 자 소 개

윤 재 한

현 아주대학교 시스템공학과 박사과정, 주로 철도 분야의 시스템 개발과 시스템 안전 확보를 위한 다수의 과제 수행. 주요 관심분야는 모델기반 시스템공학, Systems Safety, Modeling & Simulation, 기술 관리 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 팔달관 117-1호

이 재 천



현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과 공학사. KAIST 전기 및 전자공학과 공학석사 및 공학박사. 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