시스템 개념설계 단계에서 안전도 향상을 위한 시스템공학 및 시스템안전 프로세스의 통합에 관한 연구

김 영 민* · 이 재 천*
*아주대학교 시스템공학과

A Study on the Integration of Systems Engineering Process and Systems Safety Process in the Conceptual Design Stage to Improve Systems Safety

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

Abstract

Recently, we have witnessed the definitely negative impacts of large-scale accidents happened in such areas as atomic power plants and high-speed train systems, which result in increased fear for the potential danger. The problems appear to arise due to the deficiency in the design of large-scale complex systems. One of the causes can be attributed to the design process that does not fully reflect the safety requirements in the early stage of the system development because of the substantially increased complexity. In this paper, to enhance the systems safety an integrated process is studied, which considers simultaneously both the system design process and system safety process from the beginning of the system development. In the conceptual system design phase an integrated process model is constructed by analyzing the activities of both the system design and safety processes. As a case study example, an inner city train system is described with the application of the developed process. The computer simulation of the example case is followed by the result discussed. The results obtained in the paper are expected to be the basis for the future study where a detailed process and its associated activities can be developed.

Keywords : Complex Systems, Safety Critical Systems, Systems Development, Systems Engineering, Safety Degrees, Process Integration

1. 서 론

최근 일본 후쿠시마 원전사고로 인해 원자력 발전소의 안전성 대한 국민들의 불감증이 나날이 커짐에 따라 국내에서도 원자력 설계 및 운용 그리고 폐기에 이르는 시스템 전 수명주기 관점에서 시스템 안전도 향상을 위한 연구가 활발히 진행 중이다. 오늘날 개발되는 시스템들은 대형 복합 시스템의 형태로 개발되는 추세이다.

† 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2012R1A1A2009193)
† 교신저자: 이재천 교수, 경기도 수원시 영통구 원천동 산 5번지 아주대학교 시스템공학과
Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
2012년 7월 20일 접수; 2012년 8월 30일 수정본 접수; 2012년 8월 30일 게재확정

그리고 이러한 대형복합 시스템에는 고속철도, 군사 무기체계, 원자력 발전소와 같은 시스템들이 있으며 이러한 시스템으로 인한 사고가 발생 시 인명·재산 등 수많은 피해를 유발시키는 시스템을 안전 중시 시스템이라고 한다[6].

시스템공학은 시스템의 안전을 확보하기 위해서 시스템 설계 및 운용 그리고 폐기단계를 포함한 전수명주기 관점에서 위험원을 식별하고 통제하기 위해 필요한 활동들을 착수시키기 위한 과학적이고 공학적인 원리의 응용을 포함 한다[5]. 따라서 안전을 다루기에 적합한 학문이라고 할 수 있겠다.

대형 복합 시스템의 개발추세를 살펴보면, 시스템 체계의 복잡화와 기술의 고도화에 따라 높은 설계 신뢰도가 요구되고 있다. 뿐만 아니라, 대형 복합 시스템을 구성하는 체계를 구성하는 부체계의 구성도 역시 복잡도는 갈수록 증가되고 다양한 공학 분야의 융합된 형태로의 시스템으로 개발됨에 따라 기존의 각 전문 분야 엔지니어의 활동으로 바라보는 시각뿐만 아니라 개발에 고려되는 모든 측면이 체계적으로 반영될 수 있어야 한다. 따라서 대형 복합 안전중시 시스템을 설계하는데 있어서 기존의 설계 방식에 따른 전문 엔지니어를 통한 설계접근뿐 아니라 성공적인 시스템 개발이 실현되도록 다학제적 수단을 제공하고 안전 중시 시스템 개발에 확산 추세를 보이고 있는 시스템공학 접근법에 따른 체계적 설계 방법이 동시에 고려되어야 할 것이다[5]. 이를 통해, 설계단계에서 시스템안전에 직결되는 요소를 식별하고 이를 동시에 설계 과정에 반영함으로써 보다 대형복합 안전중시 시스템 설계에 대한 완결성을 갖출 수 있을 것이다.[5]

현재 대형복합 안전 중심 시스템의 안전 활동이 대부분이 상세 설계단계에서의 기능중심 안전 활동에 초점을 두었다면, 최근 안전성에 대한 패러다임은 전체 시스템 설계단계 뿐만 아니라 설계이후의 단계인 운용유지 및 폐기 단계까지 고려한 패러다임이라고 할 수 있겠다[8]. 이러한 관점에서 시스템의 전 수명주기별 그리고 계층적 관점에서 접근하는 시스템공학 접근에 따른 시스템안전 프로세스와의 통합을 통해 대형복합 안전중시 시스템 설계의 안전도 향상을 위해 매우 유용하다고 말할 수 있다.

이러한 맥락에서, 시스템공학 프로세스와 시스템 안전 활동의 통합 수행에 관한 연구가 참고문헌 [6]과 [7]을 통해 발표되었다.

참고문헌[7]에서는 요구사항 분석, 기능 분석, 합성, 그리고 시스템 분석 및 최적화를 시스템공학 프로세스로 규정하고 그에 따른 위험원 분석 기법의 동시적용을 위한 프로세스를 제시하고 있으며, 본 연구와 유사한 참고문헌[6]에서는 안전 요구사항을 설계에 반영하기 위해 시스템 수명주기와 시스템 계층에 따른 위험원 분석기법을 정의하였다. 하지만, 위의 기존 연구들은 공통적으로 시스템 수명주기 전반에 걸쳐 안전을 다루려다 보니 시스템 개발의 초석 단계인 개념설계 단계에서의 안전 활동에 대한 심도 있는 연구를 수행하지 못하였다. 따라서 본 논문에서는 모든 시스템 설계의 초석인 개념설계 단계에서 안전성 확보를 바탕으로 시스템 전체 설계 신뢰도 높이고자 시스템공학 프로세스와 시스템 안전 프로세스의 수명주기, 활동, 데이터, 인터페이스에 따른 분석 결과를 바탕으로 시스템공학 전산관리지원 도구를 통해서 개념설계 단계에서의 활용 가능한 통합 프로세스 모델을 구축을 하였다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 언급하였다. 3장에서는 통합 프로세스 구축을 위한 활동들을 명시하고 4장에서는 통합설계 환경을 구축 제시하였다. 5장에서는 구축된 통합 프로세스 모델에 대한 검증을 수행하였으며, 마지막 6장에서는 본 논문의 결과를 정리 및 요약 하였다.

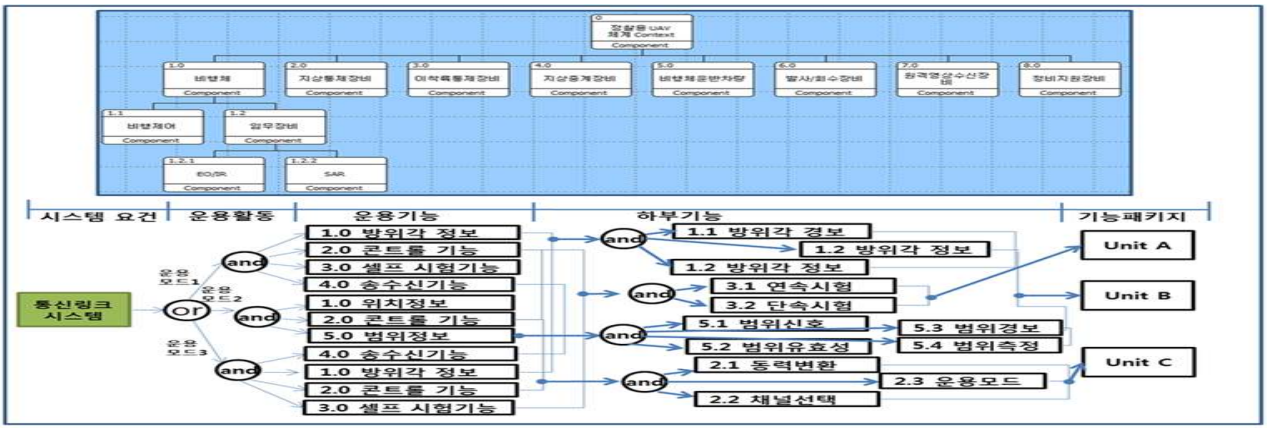
2. 문제의 정의

2.1 안전중시 시스템 설계에서 시스템공학 접근의 중요성

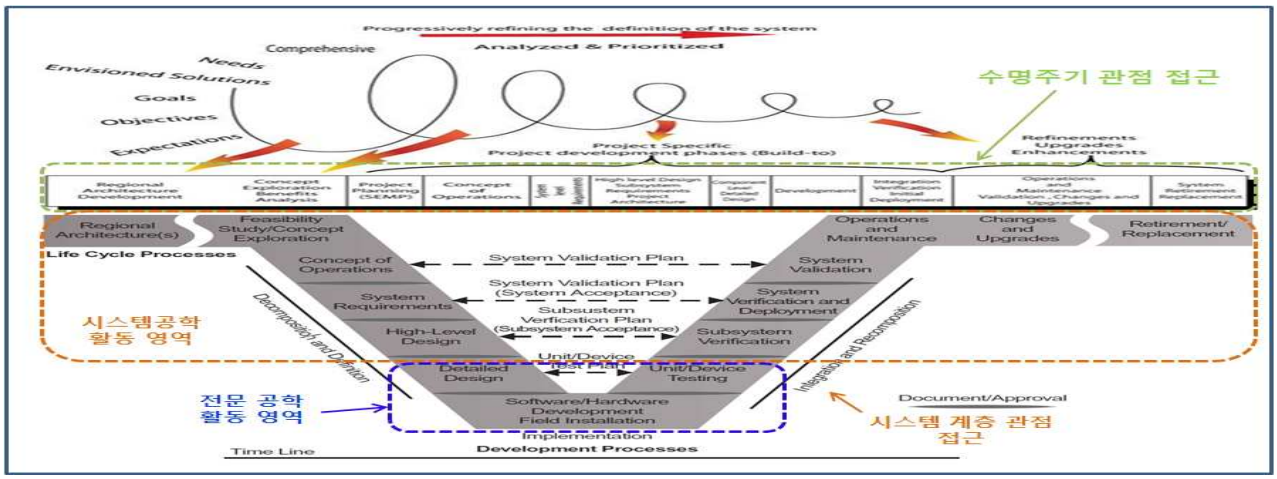
안전중시 시스템의 설계단계는 일반적으로 개념설계, 기본설계, 상세설계, 시험, 생산으로 나눠진다. 앞에서 언급한 것처럼 오늘날 대형복합 시스템의 고도화에 따른 결과, 보다 안전성이 중요히 여겨짐에 따라 <Figure 1>과 같이 보다 복잡한 부체계로 구성된 체계 개발에 대한 연구가 활발히 진행 중이다. 모든 시스템 개발단계의 초석이라고 할 수 있는 개념설계 단계에서는 본 연구에서 개발 대형복합 안전중시 시스템이 지녀야 할 운용개념과 사양(Spec.)을 바탕으로 대형복합 시스템에 탑재될 부체계의 선택에 있어서 최적화된 설계가 되도록 고려 할 것이다. 뿐만 아니라, 개발 대상인 대형복합 안전중시 시스템이 지닌 임무 및 운용 시나리오에 따른 시스템 구현이 가능한 시스템이 개발되어 질 것이다.

<Figure 1>에 대해 설명하자면, 시스템 요소에 대해 시스템 요건과 운용개념으로부터 최종적으로 Unit으로의 식별 모습을 보여준다. <Figure 1>은 통신링크 시스템에 대한 시스템 요건과 3개의 시스템 운용모드에서 운용기능이 식별된다. 식별된 운용기능은 하부기능

으로 분해된 다음 이를 기능 Set으로 묶어 개별 Unit으로 그룹화 된다. 또한 그룹화된 개별 Unit은 상호 제거 또는 교체를 하더라도 다른 Unit에 아무런 영향을 주지 않도록 설계 되어야 한다. 따라서 오늘날같이 복잡한 부체계로의 구성과 고도화된 임무수행을 위한 대형복합 안전중시 시스템의 개발단계에서 설계 신뢰성을 향상시키기 위해서는 보다 심도있는 개념설계가 필요하다. 이렇듯 상위 설계단계에서의 보다 체계화된 설계 기법을 적용하기 위해서는 시스템공학 설계 기반의 접근을 따라 수행되어져야 한다.



<Figure 1> A set of functions packages derived by analyzing the system requirements of a reconnaissance UAV

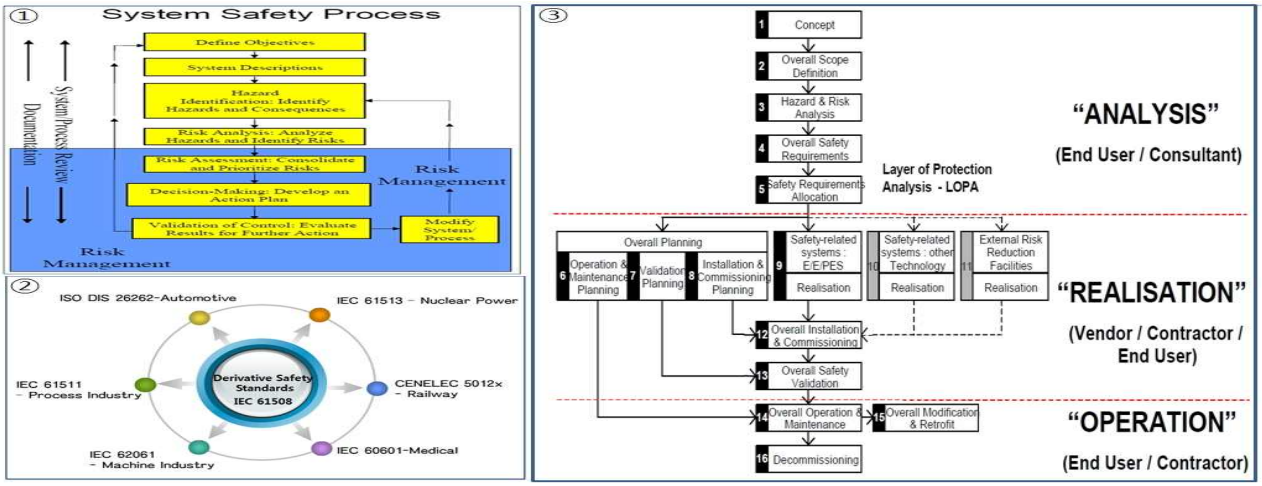


<Figure 2> V-model based on the system life cycle [8]

2.2 시스템공학 설계 프로세스와 시스템 안전 프로세스의 통합 필요성

<Figure 2>에서 보여주는 것처럼 시스템공학은 다른 전문공학 분야의 영역보다 보다 폭 넓은 수명주기 범위와 계층적 관점에서 시스템 개발 및 관리를 수행한다. 또한 시스템공학 활동의 특징은 반복적이고 점진적인 형태의 개발을 추구한다.

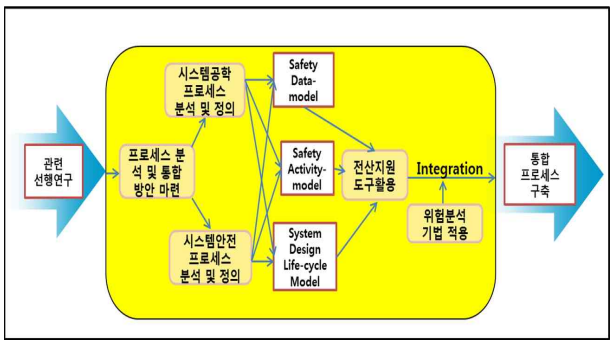
<Figure 2>의 상부는 ISO/IEC 15288[8]의 시스템 수명주기를 기술하고 있으며 하부는 Vee모델로서 각 단계에서의 개발 활동을 권하고 있다. 또한 Vee 모델의 좌측은 시스템을 계층별 세분화하며 우측은 통합 및 검증활동을 수행하고 있다. <Figure 3-①,②>에서 볼 수 있는 일반적인 시스템 안전 프로세스를 기반으로 산업에서는 별로의 표준이 재정되어 이를 적용하여 준수하고 있다. <Figure 3-③>를 통해서 볼 수 있듯이 최근 안전 분야에서도 시스템 안전을 관리하기 위해 전 수명주기 관점에서 접근하고 있다. 하지만 이러한 표준의 공통점은 시스템공학에서 주장하는 계층적 관점에서의 접근을 통한 안전 활동이 체계적으로 다루지지 못하고 있는 점이다.



<Figure 3> ① Systems safety process, ② Standards rooted on the system safety standard IEC 61508., ③ IEC 61508 safety lifecycle[4]

2.3 연구 목표 및 범위

상위 선행연구 분석을 통해 안전중시 시스템의 설계 단계에서 안전이 시스템 전수명주기와 시스템 계층분석 접근에 따른 설계가 다루어져야 한다는 것을 인지하였다. 특히 설계의 첫 단추 역할과 시스템 개발의 성공의 중추적 역할을 하는 개념설계의 중요성 인식에 따른 체계적 접근에 따른 안전성 확보를 위한 방안이 필요하다.



<Figure 4> A conceptual diagram representing the objectives of the paper

본 연구에서는 이를 위해 시스템공학 설계 표준 중 국제표준인 ISO/IEC 15288:2002을 기반으로 개념설계 단계에서의 적용을 위한 시스템공학 설계 프로세스와 시스템 안전 프로세스의 분석에 따른 통합 프로세스 모델을 제안한다. 통합 설계 프로세스는 안전 관리를 위해 필요한 정보들을 함께 정의하고 이들 간의 관계를 도식화 한다. 또한 어떠한 활동과 정보들이 언제 어떤 활동에 활용되는지 명시하도록 한다. 구축된 통합 프로세스 모델을 바탕으로 전산지원 도구를 활용해 통합 프로세스 모델의 구축 및 검증에 관한 연구를 수행하였다. 또한 통합 프로세스 구축에 대한 연구 수행 방법을 <Figure 4>를 통해서 도식화 하였다.

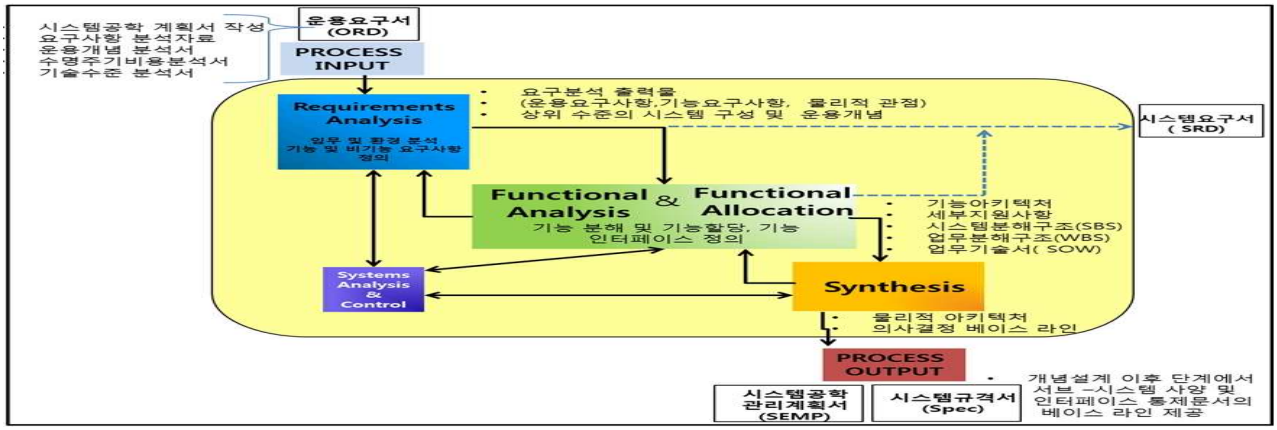
3. 프로세스 분석활동

3.1 개념설계(Conceptual Design) 단계에서의 시스템공학 설계 프로세스

본 연구의 영역은 일반적으로 시스템공학에서 말하는 크게 3가지 시스템 설계단계 중 첫 번째 단계에 해당하는 개념설계 단계이다. 각 단계의 정의는 다음과 같다[6].

1) Concept Development : 시스템의 요구를 정의하고 이를 해결할 수 있는 여러 대안에 대한 검토 및 근거를 바탕으로 하나의 대안을 선택하는 과정.
2) Engineering Design : 선택된 대안을 바탕으로 물리적 설계가 이루어지는 단계.
3) Post Engineering : 시스템의 설계완료 후 사용자의 사용에 대하여 지원 및 폐기에 관한 단계.

또한 본 연구진은 앞선 연구활동 참고문헌[9]를 통해 개념설계란 시스템 설계 프로세스 초기의 한 부분으로서 사용자가 요구사항을 개념적 모델로 변환하는 단계로 바라보고 있다. 개념설계 단계에서 요구되는 시스템 공학 설계 활동을 다음과 같이 규정하였다.



<Figure 5> The process for the conceptual design phase in the domestic defense R&D [9]

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

따라서 위에서 언급한 개념 설계 시 요구되는 시스템공학 활동들을 개념설계 단계의 프로세스로 규정하고 개념설계 단계의 프로세스 구성 및 산출물을 나타낸 모식도를 <Figure 5>와 같이 나타내었다. <Figure 5>를 통해서 알 수 있듯이 프로세스의 입력으로 들어가는 운용요구서(Operational Requirements Document, ORD)가 개념설계 프로세스를 통한 기술적 변환을 통해 최종적으로 시스템 규격서(Spec.)을 생성하는 모습을 볼 수 있으며, 개념설계 단계를 통해 시스템의 Top-Level 기능, 성능, 인터페이스를 정의 할 수 있다. 또한 기능 베이스라인의 기준으로 활용 될 수 있기 때문에 개념설계 단계에서의 산출물은 안전 활동의 중요한 단추를 제공하는 첫 걸음이다.

3.2 시스템 안전 프로세스 분석

시스템 안전의 대표 참고문헌[7]에서는 시스템 안전 프로세스를 아래와 같이 총 8단계의 프로세스 업무(Task)로 접근하고 있으며 상위 5단계의 Task가 개념설계 단계에서의 활동으로 포함된다.

1. System Safety Program Plan(SSPP)

SSPP는 시스템 안전 프로세스에 요구되어 계획되어 있는 업무와 활동에 대한 자세히 기술 되어야 한다. 이러한 SSPP의 목적은 시스템 안전 분석의 방향을 확립하며 다음과 과 같은 활동이 수반되어져야 한다.

1) Defining safety requirements
2) Detailing safety analysis techniques
3) Outlining hazard risk and assessment criteria
4) Preliminary Hazard List(PHL)

위의 PHL을 통해 대상 시스템에 대한 상위 레벨에서의 위험원이 정의된다. PHL의 목적은 시스템의 위험원에 대한 최초 식별이라고 할 수 있다. PHL의 수행에 있어서 입력 데이터는 다음과 같다.

1) Safety/system engineers from respective systems
2) Preliminary requirements and specifications
3) Generic hazards list
4) Similar Systems Hazard Analysis/lessons learned
5) Accident/Incident Reports

2. Preliminary Hazard Analysis(PHA)

개발의 초기단계에서 시스템 레벨에서의 안전 이슈(위험원)를 식별하기 위한 상위 수준에서의 예비 활동이다.

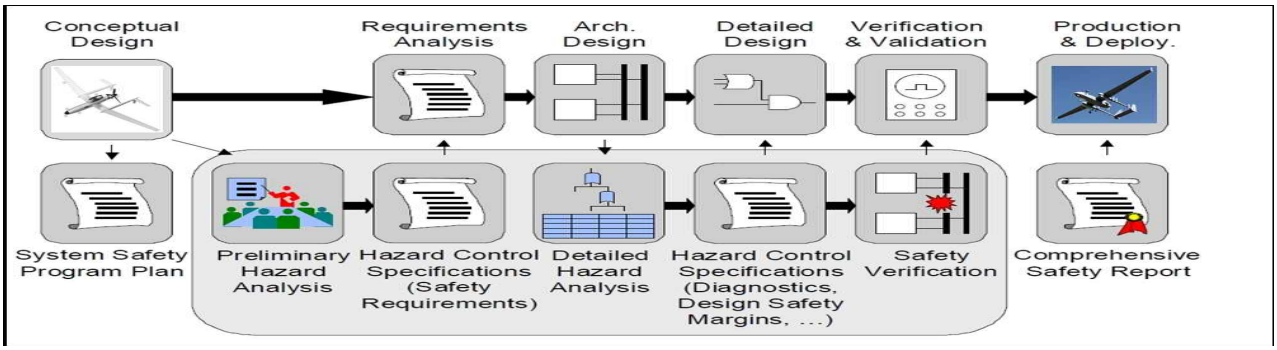
3. Subsystem Hazard Analysis(SSHA)

서브시스템에 포함된 안전요구사항을 서브시스템이 준수하는지 검증하기 위해 SSHA를 수행하며 서브시스템의 설계와 연관된 알지 못하는 위험원을 조기에 식별하기 위해 수행한다.

4. System Hazard Analysis(SHA)

다음과 같은 목적을 기반으로 수행되어진다.

1) 시스템 사양에 포함된 안전 요구사항을 준수하는지 시스템을 검증하기 위해서 SHA 수행



<Figure 6> An example case of how the system safety process can be carried out

2) 서브시스템 인터페이스와 시스템 기능 오류와의 연관된 식별되지 않은 위험원을 인지
3) 소프트웨어, 서브 시스템 인터페이스를 포함한 전체 시스템 설계와 연관된 식별되지 않은 위험을 인지하기 위해서 수행

SHA를 수행하기 위한 위험분석 기법으로 다음과 같다.
1) FTA(Fault Tree Analysis)
2) FMEA(Failure mode and effects analysis)
3) ETA(Event tree analysis)
4) RHA(Radiation hardness Assurance)
5) Interface Analysis

5. Operating and Support Hazard Analysis
O&SHA는 운영적 절차와 지원 절차의 활동에 대한 평가를 통해 시스템의 생산. 배치, 설치, 운영, 유지보수에 관한 시스템 안전성 평가를 문서화 한다.

6. Hazard Tracking and Risk Resolution

7. Safety Assessment Report

<Figure 6>은 시스템 안전 프로세스와 설계 프로세스가 어떠한 연관이 있는지를 보여준다. 하지만 <Figure 6>을 통해서는 개념설계 단계에서의 세부 프로세스에 따른 주명주기와 계층적 접근에 따른 안전활동에 있어서 큰 제약이 따른다. 따라서 본 연구를 통해 이러한 문제를 개선하고자 한다.

4. 통합 설계 모델의 구축

4.1 프로세스의 활동 및 입·출력물 분석

모든 존재하는 프로세스에는 입·출력물이 존재하기 마련이다. 한 예로, 하나의 프로세스에 대한 입력물은 프로세스 과정을 거쳐 출력물을 생성하지만, 이는 다음 프로세스의 입력으로도 활용될 수 있다는 점에 주의해야한다. 이러한 맥락에서 실제 설계 프로세스와 시스템 안전 프로세스의 활동에 따른 데이터 산출물의 상호 관계와 흐름이 설계단계에서의 안전성 확보에 매우 중요한 요소가 될 수 있다. 따라서 본 연구영역인 개념설계 단계의 전·후 프로세스와도 프로세스 및 산출물의 상호 영향도 분석을 수행하였다.

일반적으로 개념설계의 전 단계를 예비 개념설계 단계(Pre-Conceptual Design, PCD)라 칭한다. PCD 단계에서의 시스템공학 설계 활동은 임무분석에 따른 임무요건이 생성된다. 생성된 임무요건을 바탕으로 개념설계 단계가 수행됨에 따라 중요한 활동이지 않을 수 없다. PCD 단계에서 시스템 안전 활동으로는 우선, 안전 활동 목적 설정에 따른 범위 설정이 되어야 한다.

확정된 범위를 통해, 시스템 설계에 요구되는 전반적인 안전 활동 계획이 수립된다. PCD 단계에서도 개념설계 단계로의 진입 전에 위험원 식별, 예비 개념 위험원 분석 및 분류를 수행하여 그에 따른 결과 반영에 의해 설계단계에서의 안전에 관한 전략을 재수정하게 된다.

개념설계단계(Conceptual Design, CD)에서는 PHA를 통해 시스템개발의 초기단계에서 시스템 레벨에서의 위험원을 식별하기 위한 상위 수준에서의 예비 활동을 수행한다. 따라서 PHA를 기반으로 분석된 결과를 바탕으로 안전 요구사항이 생성된다. 이렇게 생성된 안전 요구사항이 설계단계에 반영되기 위해서 개념설계 단계의 요구사항 분석활동에 반영되어 야 한다. 따라서, 이해당사자 요구사항을 정의하기 위해서 PHL, PHA, SSHA를 통해 수행되어진다[8].

시스템공학 개념설계 프로세스의 두 번째 해당하는 기능분석·할당 단계에서는 기능아키텍처를 통해 안전기능과 안전요구사항을 도출할 수 있다. 또한 시스템공학 설계 프로세스의 통합단계의 수행을 통해 물리적 아키

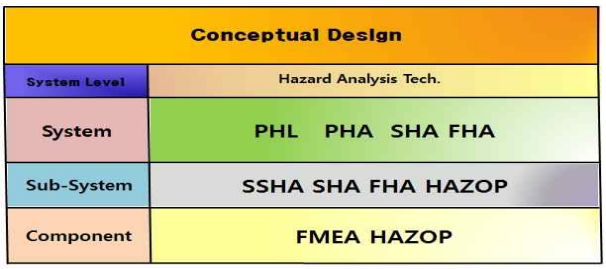
텍처 설계가 이루어 진다. 이러한 아키텍처 설계를 바탕으로 보다 상세한 위험원 분석이 가능해진다.

앞에서 언급한 것처럼 시스템공학 설계프로세스는 반복·순환구조의 프로세스 수행을 통해 점진적 개선된 설계를 추구한다. 따라서 이러한 관점에서 개념설계 단계를 구성하는 프로세스의 진행에 따라 안전 활동 역시 보다 상세화 된다는 것을 알 수 있다.

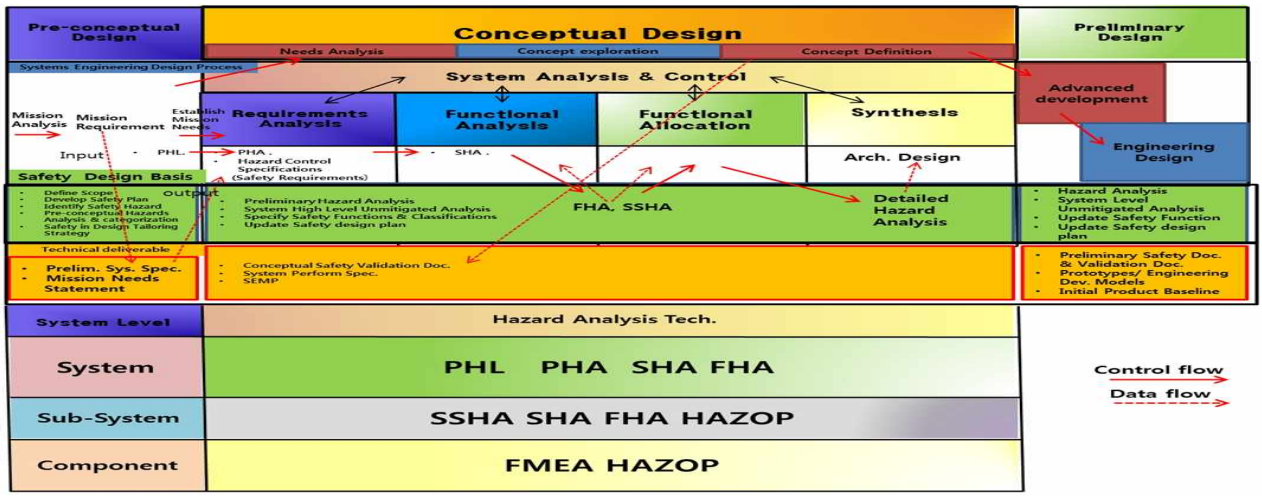
앞에서 정의한 CD단계를 거쳐 도출된 시스템 기능 사양(Spec.)과 시스템 개념을 바탕으로 개념설계의 이후단계인 Engineering Development 단계에서는 보다 상세화된 물리적 구현을 통해 위험분석 활동, 안전기능에 대해 보다 구체화해 나아간다. 이를 통해 개선된 사항은 안전 설계 계획의 조정을 통해 반영되어진다.

4.2 계층적 관점에서의 안전 활동 분석

시스템공학의 프로세스는 시스템, 서브시스템, 컴포넌트 순으로의 계층적 관점에서의 접근을 중요시 한다. 따라서 시스템의 안전을 추구하기 위해서 안전 활동에 대한 계층적 분석이 이루어져야 한다. 앞서 언급된 연구내용을 바탕으로 <Figure 8>과 같이 정리 하였다. 시스템 레벨에서는 PHL, PHA, SHA, FHA를 통한 안전 활동이 이루어져야 할 것이다. 기능 위험원 분석(FHA)는 단독으로 수행되지 않고 PHA나 SSHA와 같은 다른 위험원 분석들과 함께 수행되어야 한다[8]. SHA는 보통 SSHA가 거의 완료되었을 때 수행한다[8]. 또한 SHA는 시스템 통합의 결과물을 기반으로 상세 위험원을 분석하는 활동이다. 따라서 인터페이스 관련 위험원이 하위 시스템 인터페이스 정보를 기반으로 SSHA에서 예비 분석되고 인터페이스 기술서를 기반으로 SHA에서 자세히 분석된다. 또한 SHA는 아키텍처 설계 프로세스와 함께 수행 되어야 한다.



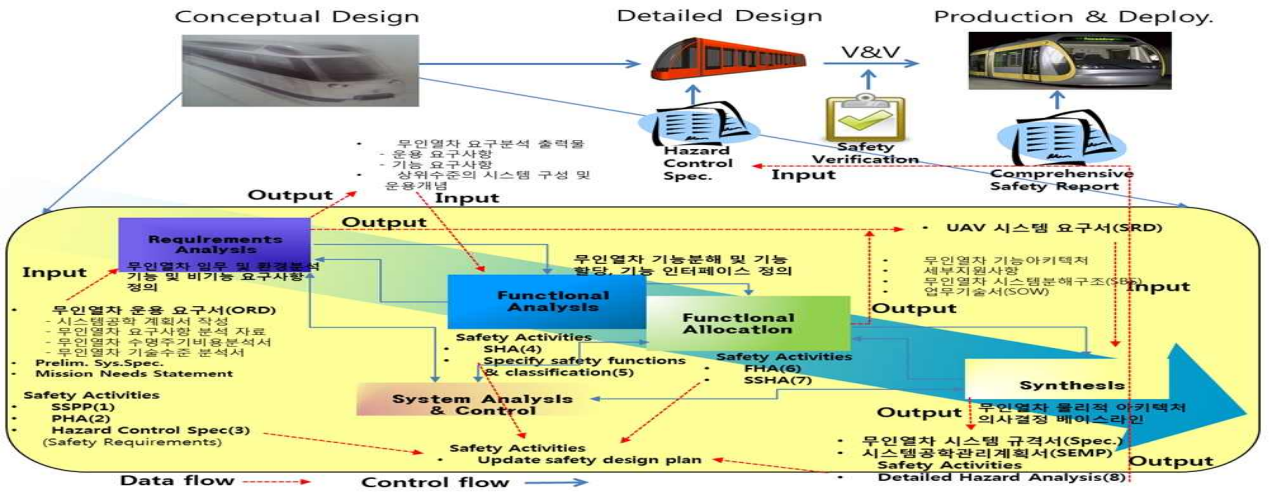
<Figure 7> Safety activities performed at each system layer



<Figure 8> The integrated process model under study

4.3 구축된 통합 프로세스 모델

<Figure 8>를 통해 제시한 것처럼 프로세스 통합 모델을 구축하기 위해서 시스템공학 설계 프로세스와 시스템 안전 프로세스에 대해 동일한 수명주기 기준을 가지고 개별 프로세스의 분석을 통해 활동 및 산출물을 명시하였다. 또한 활동(Activity)에 따른 입·출력되는 산출물들의 관계를 제시하여 설계변경에 따른 영향도 분석이 가능하게 하였다. 이밖에 설계대상 시스템의 개발단계의 해당 수명주기와 계층구조에 따른 위험분석이 가능해졌다. 구축된 통합 프로세스 모델의 흐름이 논리적인 흐름으로 진행되고 있는지 평가하기 위해 시스템공학 전산지원도구의 EFFBD(Enhanced Functional Flow Block Diagram)를 통해서 프로세스 모델을 구현하였다.



<Figure 9> Application of the integrated process model in the design of a train system operated without drivers

5. 구축된 통합 설계 프로세스 모델의 검증

5.1 무인화 열차 시스템 설계의 적용 사례

5.1.1 대상시스템의 개요

최근 열차 시스템은 기관사가 없이 사전에 입력된 프로그램을 따라 열차가 스스로 자율운행을 하는 무인화 시스템 운행을 해야하기 때문에 매우 복잡한 부체계로 구성되어 있다. 따라서 제어시스템에 대한 설계 신뢰도가 시스템 운용과 설계 안전도에 큰 영향을 미친다. 제어시스템 복잡도와 기능의 고도화로 인해 기존 유인 열차와는 다른 개념의 제어기술이 개발되어야 한다. 따라서 새로운 개념의 시스템의 체계적 개발을 통한 설계 안전도 향상을 위해 본 논문에서 제안하는 통합 프로세스 모델을 따라 대상 시스템인 무인열차 시스템에 적용 하였다.

5.1.2 대상시스템에 대한 적용

개념설계 단계의 무인화 열차 시스템설계에 있어서 <Figure 8>에 정의된 통합 프로세스 모델을 적용 시켰다. 개념설계를 구성하는 서브 프로세스 5가지에 대해 개별 프로세스에서 요구되어 수행되어야 하는 활동, 그리고 활동에 따른 산출물, 산출물의 입·출력 관계, 수행되어야 하는 안전 활동의 식별 및 수행 순서를 <Figure 9>와 같이 적시하였다.

개념설계 단계에서는 상위수준의 안전활동이 이루어진다. 따라서 대부분의 안전활동이 요구사항 분석 단계에 적용되며, 무인열차 운용 안전 요구사항, 기능 안전 요구사항 등이 도출된다. 이러한 안전 관련 요구사항을 바탕으로 안전 기능 식별과 기능 위험분석을 통해 기능할당 및 기능 인터페이스를 정의하였다. 요구사항 분석 단계에서 산출된 무인열차 운용 요구서와 기능 분석 및 할당 수행을 통한 산출물로 무인열차 시스템 요구서를 작성하였다. 개념설계 단계의 통합프로세스는 무인열차 시스템 요구서를 바탕으로 최종적 시스템 규격서(Spec.)를 생성하게 된다.

기존의 개념설계 단계에서 시스템공학 설계 프로세스와 시스템안전 프로세스의 개별 수행에 따른 결과보다 체계적인 무인열차 시스템의 개념설계 단계에서의 활동을 통해 시스템 안전도 향상을 기대할 수 있겠다.

5.2 전산지원 도구를 통한 모델 시뮬레이션

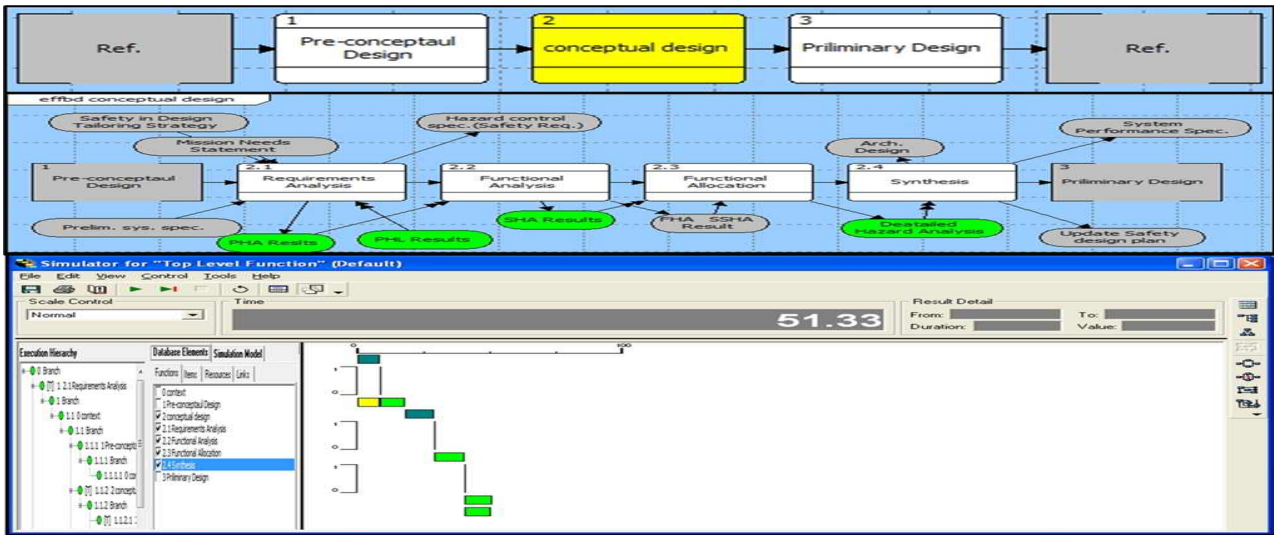
5.2.1 시뮬레이션 대상 및 범위

본 연구결과에 대한 검증수행으로 시뮬레이션을 수행하였다. 앞에서 언급한 것처럼 프로세스에 존재하는 입·출력물은 다음 진행 프로세스에 영향을 끼칠 수 있다.

따라서, 본 논문에서의 시뮬레이션 대상은 아래 <Figure 10>에 제시한 바와 같이 개념설계 단계와 전·후 설계단계인 PCD와 PD 설계단계를 포함한다. 또한 대상에 대한 시뮬레이션 범위를 통합 설계 프로세스 모델의 연구범위인 개념설계로 한정하며, CD단계의 프로세스 뿐만 아니라. PCD와 PD단계로부터 입력되는 데이터를 모두 고려하였다.

5.2.2 시뮬레이션 결과

<Figure 10>과 같이, 개념설계 단계의 프로세스를 구성하는 서브-프로세스 4개(요구사항 분석, 기능분석, 기능할당, 통합단계)와 각각의 개별 프로세스로의 입 · 출력 요소 12개에 대해 시뮬레이션에 반영하였다.



<Figure 10> Verification of the resulting integrated process model by computer simulation

프로세스에 대한 시간선 분석의 시뮬레이션 수행결과 <Figure 10>의 왼쪽하단에 보이는 것과 같이 Branch에서의 흐름뿐 아니라 개념설계를 구성하는 모든 흐름에서 녹색표시를 볼 수 있다. 또한 <Figure 10>의 그림 오른쪽 하단을 통해서 서로 다른 색으로 구성된 바의 형태의 막대기가 51.33이라는 시간선 지표를 나타내는 것을 볼 수 있다.

5.2.3 시뮬레이션 결과의 해석

<Figure 10>의 왼쪽 하단의 그림을 통해 Branch 마다의 흐름에서 녹색 원의 표시를 볼수 있다. 이는 프로세스의 구성이 원활이 진행해고 있다는 것을 나타내며, <Figure 10> 아래의 오른쪽에 나타난 연두색의 바는 프로세스 상에서 트리거 데이터의 도착 후 원활히 기능이 이행되었다는 것을 보여준다. 또한 노락색 바의 경우는 트리거 데이터의 도착을 기다리기 위해서 아직 실행되지는 않은 기능이나 프로세스 흐름에는 지장을 주지 않는다는 것을 의미한다. 따라서 본 연구를 통해 구성된 통합 프로세스 모델이 시뮬레이션 시간선 분석에 따라 가장 작은 값에서 원활한 프로세스의 흐름값을 보였던 시간값 53.33에서 통합 프로세스 모델에 대한 최적화를 마쳤다. 앞에서 언급된 바와 같이 통합 프로세스 모델이 실제 흐름에 충돌 없이 잘 수행되는지 파악하고, 각 프로세스 활동의 수행 시기가 서로 원하는 시기에 수행 되는지 전산지원도구를 통해 확인하였다. 앞에서 언급한 시스템공학 전산지원 도구인 CORE ® 툴을 통해 검증 가능한 모델링 기법인 EFFBD를 활용한 Time-Line analysis을 통해 시뮬레이션을 수행하였다. 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 올바르게 수행되고 있음을 확인하였다.

6. 결론 및 요약

오늘날 대형 복합 시스템의 등장으로 우리사회에 여러 편의를 도모하고 있지만 시스템의 고도화와 복잡화 추세로 개발 및 운용에 있어서 많은 어려움 뿐만 아니라 사고 발생시 많은 위험을 발생 시킨다. 따라서 미래의 대형복합 안전중시 시스템 개발에서는 현재보다 높은 설계 신뢰도가 요구되어야 할 것이다.

따라서 본 연구 수행을 통해서 대형복합 안전중시 시스템 개발 사업에 있어서 보다 체계적으로 설계에 접근할 수 있는 시스템공학 프로세스에 의한 설계접근과 체계적인 시스템 계층관점에서의 접근의 설계방식, 시스템 안전 설계프로세스, 그리고 위험 분석 기술의 통합된 구축 모델 개발을 통한 개발사업을 통해 향후 보다 개선된 설계 신뢰도를 갖춰 안전중시 시스템의 안전성을 확보할 수 있을 것이다.

본 연구에서는 ISO/IEC 15288:2002의 시스템공학 설계프로세스와 시스템 안전 프로세스에 대해서 개념설계 단계에서의 수명주기, 활동, 데이터, 인터페이스에 관한 분석을 통해서 통합 모델을 개발하고자 노력하였다. 그밖에 위험분석 기법에 대한 적용시기 및 적용 시스템 계층을 명시함에 따라 본 연구결과를 바탕으로 대형복합 안전중시 시스템의 설계를 수행한다면, 상위

수준에서의 시스템 설계 활동 및 안전 활동을 동시에 고려한 설계 활동이 가능해짐에 따라 안전중시 시스템의 개발 사업관리 측면의 활용적 가치에 기여하였다고 생각 한다. 따라서 후속 연구 활동 또한 활발히 진행되었으면 한다. 추후 연구에서는 연구범위를 확장시켜 안전중시 시스템 설계에서 보다 개선된 설계 프로세스를 제시하는 연구가 필요할 것이다.

7. 참 고 문 헌

[1] A. Kossiakoff and W. N. Sweet, Systems Engineering Principles and Practice. New Jersey: Wiley, 2003, pp. 117-138.
[2] “A guide for system life cycle processes and activities INCOSE.”, handbook, c3.2, (2010)
[3] DoD, “Standard Practice for System Safety: ESOH Risk Management Methodology for Systems Engineering” in MIL-STD-882D, (2000)
[4] “Functional safety of electrical/electronic/programmable electronic safety-related systems“, in IEC 61508
[5] I. Clifton and A. Ericson, “Hazard analysis techniques for system safety.”, Hoboken, New Jersey: John Wiley & Sons, Inc., (2005)
[6] J. H. Yoon and J. C. Lee, “A Process Model for the Systematic Development of Safety-Critical Systems,” Korea Safety Management & Science, vol. 11, pp. 19-26, (2009)
[7] J. Y. Park and Y. W. Park, “Model-based concurrent systems design for safety,” Concurrent Engineering-Research and Applications, vol. 12, pp. 28-294, (2004)
[8] Systems Engineering - System life cycle process, in ISO/IEC 15288:2002(E): International Organization for Standardization, (2002)
[9] Y. M. Kim and J. C. Lee, “On the Use of SysML Models in the Conceptual Design of Unmanned Aerial Vehicles,” Korea Information & Communication Society, vol. 37, pp. 206-216, (2012)

저 자 소 개

김 영 민

현 아주대학교 시스템공학과 석·박사통합과정. 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