데이터모델 관점에서의 시스템설계 및 시스템안전 프로세스의 통합에 관한 연구

김 영 민* · 이 재 천*
*아주대학교 시스템공학과

On the Integration of Systems Design and Systems Safety Processes from an Integrated Data Model Viewpoint

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

Abstract

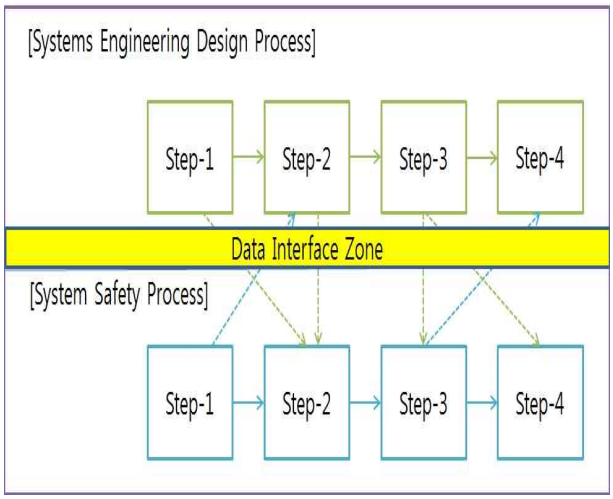
The issues raised so far in the development of safety-critical systems have centered on how effectively the safety requirements are met in systems design. The systems are becoming more complex due to the increasing demand on the functionality and performance. As such, the integration of both the systems design and systems safety processes becomes more important and at the same time quite difficult to carry out. In this paper, an approach to solving the problem is presented, which is based on an integrated data model. To do so, the data generated from the inputs and outputs of the systems design and systems safety processes are analyzed first. The results of analysis are used to extract common attributes among the data, thereby making it possible to define classes. The classes then become the cores of the interface data model through which the interaction between the two processes under study can be modeled and interpreted. The approach taken has also been applied in a design case to demonstrate its value. It is expected that the results of the study could play a role of the stepping stone in extending to the architecture development of the integrated process.

Keywords : Systems Engineering, Systems Design, Systems Safety, Data Models, Attributes, Classes, Interface Models, Safety-Critical Systems

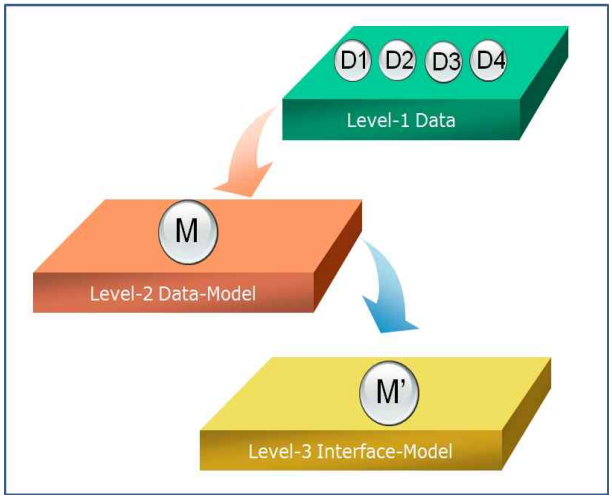
1. 서 론

현대사회에서 개발되는 대부분의 시스템은 대형 복합체계로 구성된 형태를 보이고 있다. 따라서 시스템을 구성하는 하부 시스템인 개별 서브-시스템의 성공적인 개발에도 불구하고도 개발된 시스템을 통합하는 과정에서 수많은 오류로 인해 개발비용 상승 및 일정지연 등 막대한 영향을 끼쳐 연구개발 단계에서 많은 어려움을 주고 있다. 이러한 문제의 근본적인 이유는 대형 복합 시스템을 구성하는 하부 시스템간의 데이터 연동과 관련한 인터페이스가 차지하는 비중이 나날이 급증하고 있기 때문이다.

† 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 10월 19일 접수; 2012년 11월 30일 수정본 접수; 2012년 12월 7일 게재확정



<Figure 1> A view on a virtual zone for interfacing between the systems design and systems safety processes



<Figure 2> Mapping from a Data or a Model-Model to an Interface-Model

따라서 대형 복합시스템 설계단계의 통합과정에서 인터페이스로 인한 수많은 문제가 야기됨에 따라 시스템을 구성하는 하부 시스템들 간의 상호 운용성(Interoperability) 측면 등 여러 방안을 통해 인터페이스로부터 발생되는 문제를 해결하기 위해 다각도로 연구가 활발히 진행되고 있다.

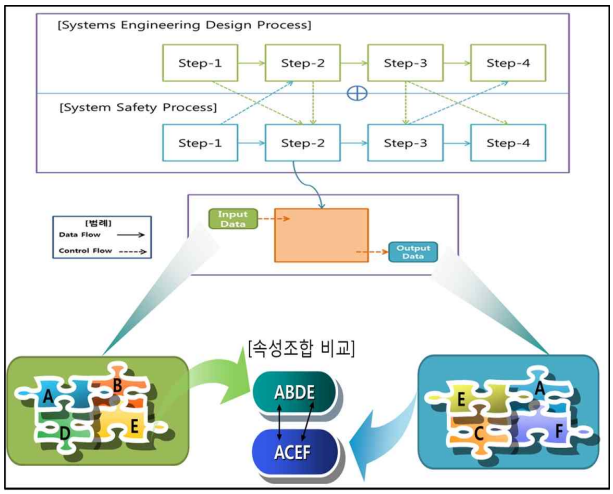
최근 세계 곳곳에서 원자력 발전소와 고속열차로부터 발생한 사고로 안전 중시 시스템에 대한 안전대책에 관해 시급히 재조명 되고 있다. 안전 중시 시스템이란 시스템으로 인한 사고가 발생 시 인명·재산 등 수많은 피해를 유발시키는 시스템을 일컬으며 이러한 시스템에는 고속철도, 군사 무기체계, 원자력 발전소와 같은 대형 복합시스템들이 이에 속한다[3].

안전중시 시스템의 전 수명주기 설계단계에서 시스템안전 활동과의 상호 유기적인 인터페이스관계를 동시에 고려한 설계활동을 통해 시스템 안전도 향상을 위한 노력이 수행되어져야 할 것이다. 현재 대형복합 안전 중심 시스템의 안전 활동이 대부분, 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[2][7]. 이러한 관점에서 시스템의 전 수명주기별 그리고 계층적 관점에서 바라보는 시스템공학에 따른 접근은 매우 유용하다 말할수 있겠다[4]. 따라서, 시스템공학 프로세스와 시스템안전 프로세스와의 통합을 통해 보다 개선된 대형복합 안전중시 시스템 설계의 안전도 향상을 추구할 수 있을 것이다.

관련 주제에 대한 연구가 최근에 선행연구 [5],[6],[9]에 발표 되었다. 선행연구 [5]에서는 요구사항 분석, 기능 분석, 합성, 그리고 시스템 분석 및 최적화를 시스템공학 프로세스로 규정하고 그에 따른 위험원 분석 기법의 동시적용을 위한 프로세스를 제시하였다. 또한, 선행연구 [6]에서는 철도 시스템 개발에서 수명주기에 따른 시스템공학 프로세스와 안전성 평가를 동시에 고려한 통합 프로세스를 제시하였다. 선행연구 [9]을 통해, 개념설계 단계에서의 시스템 수명주기와 계층 수준에 따른 시스템공학 설계 프로세스와 시스템 안전 프로세스의 활동과 활동에 따른 입·출력 데이터 분석을 통해 통합 설계 프로세스 모델을 제시하였다.

하지만, 기존연구를 통해서는 개념설계 단계에서의 시스템공학 설계 프로세스와 시스템 안전 프로세스의 수행에 따라 발생하는 데이터의 상호 유기적인 인터페이스 식별을 제시하였다고 보기 어렵다. <Figure 1>에서 제시한 것처럼, 시스템공학 설계프로세스와 시스템 안전 프로세스 수행에 따른 산출물 사이의 상호 유기적인 데이터 공유가 존재함을 생각해 볼 수 있다. 따라서, 시스템과 시스템을 구성하는 하부 시스템의 통합과정에서만 인터페이스 측면을 다루기보다 이러한 설계와 안전활동의 초석이라고 할 수 있는 시스템공학 설계 프로세스와 시스템 안전 프로세스 사이의 인터페이스 측면을 다루어 보다 실제적인 시스템 안전도를 향상 시킬 수 있도록 두 프로세스 간의 데이터 중심의 통합 인터페이스 모델을 구축하였다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 3장에서는 시스템공학 설계 프로세스와 시스템안전 프로세스의 통합된 프로세스 모델을 바탕으로 인터페이스



<Figure 3> Comparison of data attributes from the inputs and outputs of the processes

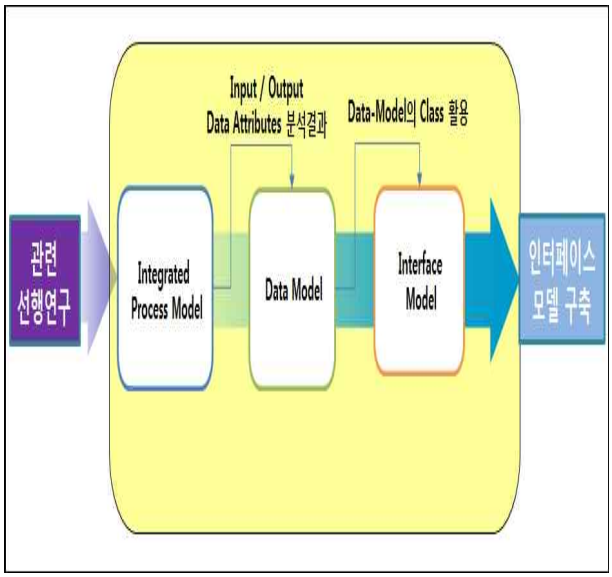
모델 구축을 위한 활동들을 명시한다. 4장에서는 인터페이스 모델 구축 환경을 제시하였다. 또한, 5장에서는 구축된 인터페이스 모델에 대한 검증을 수행하였으며, 마지막 6장에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 문제의 정의

2.1 데이터-모델 생성을 통한 인터페이스 모델 개발의 필요성

모델이란 사전적 의미로 대상물을 이해하기 쉽게 혹은 취급하기 쉬운 형태로 표현한 것을 말한다.

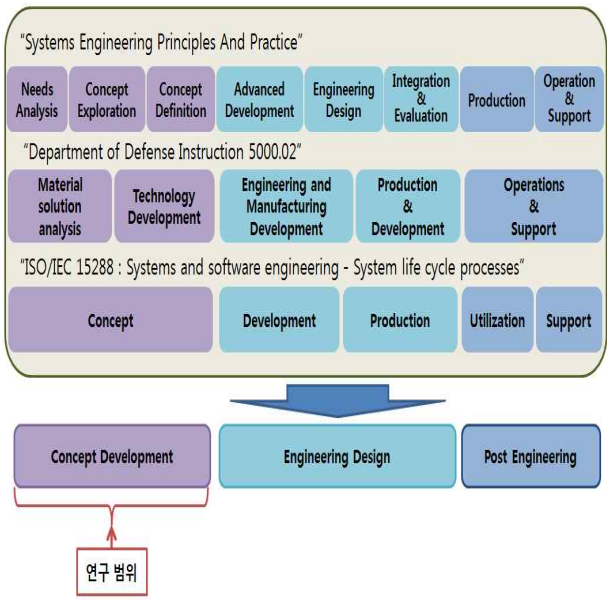
따라서 본 연구에서 대상으로 다루는 시스템공학 설계 프로세스와 시스템 안전 프로세스를 수행함에 있어서 수없이 많이 발생하는 프로세스 입·출력 데이터에 대해 UML(Unified Modeling Language)[8]의 Class Diagram로 표현함으로써 수많은 정보를 간결한 형태로 전달할 수 있다. Class Diagram은 기본적으로 Class의 거동과 속성을 기술한다. 또한, Class Diagram은 구성하는 Class라는 개별 객체들을 모델링함으로써 객체들 간의 관계를 나타내고 객체들이 무엇을 하고 어떠한 서비스를 제공하는지를 설명한다. 특히, 본 연구 수행에 있어서 접근 방법으로 활용하려고 하는 클래스 다이어그램은 프로세스 수행에 따른 산출물의 공통 특성에 따른 클래스의 타입을 정의하고 데이터들 사이의 관계를 규정한다. 따라서 프로세스 수행과 동시에 발생하는 수많은 데이터들 간의 상위 개념적 수준에서의 상호 인터페이스 측면을 정립하는데 유용하게 활용될 수 있다.



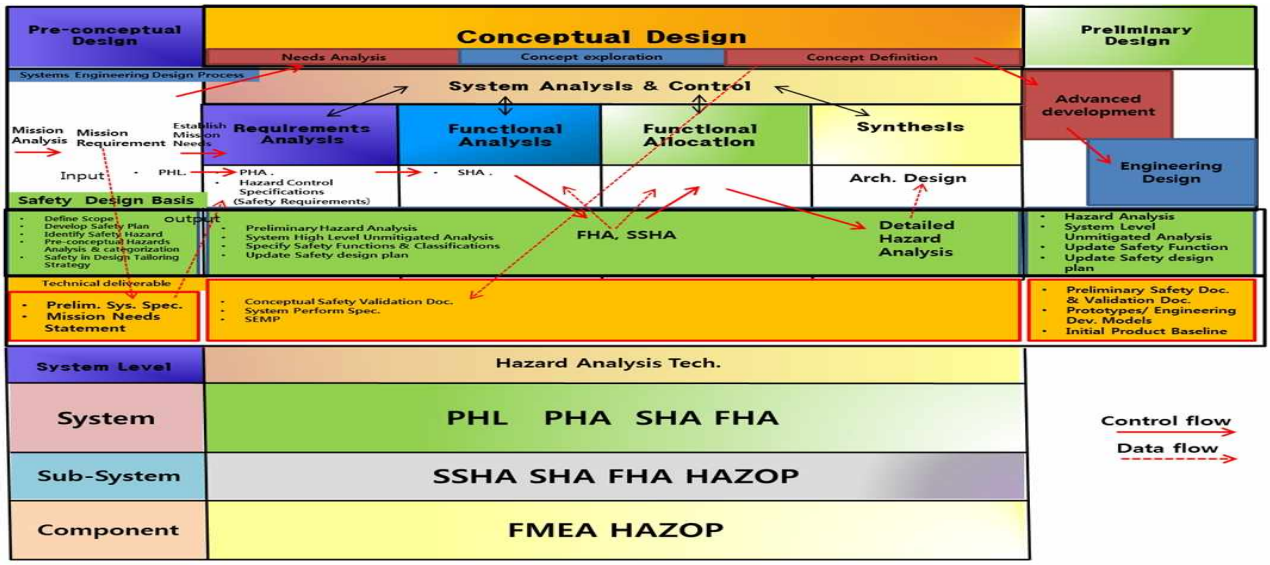
<Figure 4> A conceptual diagram representing the objectives of the paper

또한 이렇게 생성된 클래스 다이어그램은 아키텍쳐 측면에서 구성하는데 필요한 정보들과 그들 간의 관계를 정의하여 모델링하기 때문에 이러한 클래스 다이어그램은 통합 프로세스 모델에 대해 데이터 인터페이스 측면의 아키텍처를 제공함으로써 이해당사자로 하여금 공통의 이해 및 일관성을 확보할 수 있다.

2.2 데이터 속성 기반의 인터페이스 모델 생성의 중요성

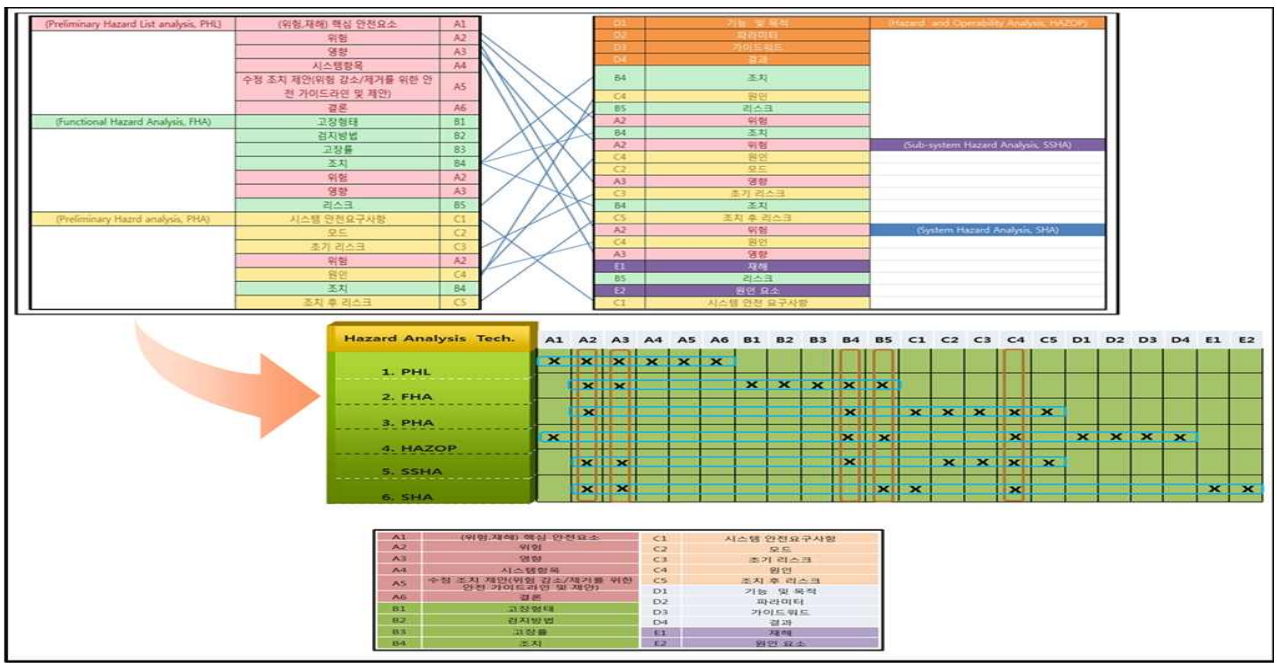


<Figure 5> System Life-cycle models

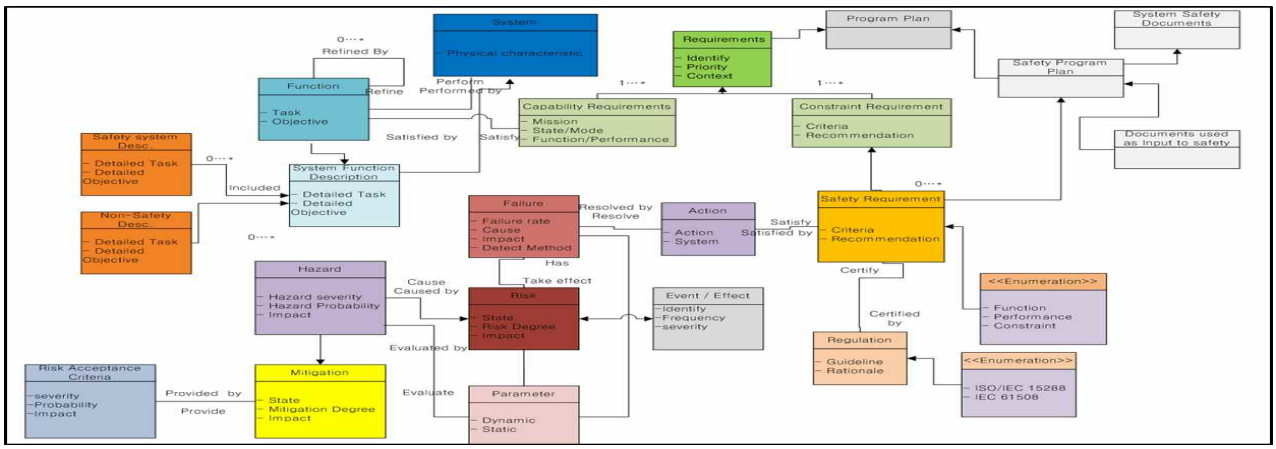


<Figure 6> The integrated process model related to the current study[7]

<Figure 6>의 통합된 프로세스 모델은 < Figure 6>에서 보여주는 것처럼 시스템공학 설계 프로세스와 시스템 안전 프로세스와 통합되어 생성된 모델이다. 또한, <Figure 3>처럼 각각의 프로세스의 진행에 따른 개별 산출물은 고유의 속성을 지니고 있다. 특히, 시스템 안전 프로세스 수행에 따른 시스템 위험분석 활동으로부터 생성된 산출 데이터의 적지 않은 부분에서 공통된 속성을 지니고 있다. 또한 이렇게 산출된 데이터의 존재의 이유가 해당 프로세스 단계만을 위한 것이 아니라 이후의 프로세스에서 또는 시스템공학 설계 프로세스와 시스템 안전프로세스 사이에서 상호 유기적인 영향을 미친다. 따라서 현대 사회에서 주로 개발되는 대형복합 시스템 설계과정에서 데이터 속성을 기반한 인터페이스 모델은 설계 단계의 참조 모델로서 활용함으로써 보다 체계적인 설계 접근을 통해 시스템 안전도 확보를 위한 보다 효과적인 방안중 하나로 추구할 수 있다.



<Figure 7> Analysis of the artifacts obtained by carrying out the activities of systems design and systems safety processes



<Figure 8> The resultant integrated data model representing the interaction between the systems design and systems safety processes

2.3 연구 목표 및 범위

상위 선행연구 분석을 통해 안전중시 시스템의 설계 단계에서 상호 유기적인 영향을 미치는 데이터 속성 분석을 바탕으로 상위 수준인, 개념수준의 데이터 모델의 개발과 데이터 모델을 바탕으로 보다 상세화된 인터페이스 모델 개발을 통해 시스템 설계가 다루어져야 한다는 것을 인지하였다. 특히, 시스템 설계 단계의 초석인 개념설계 단계의 중요성 인식에 따른 체계적 접근을 통한 안전성 확보 방안이 필요하다.

본 연구에서는 기존 연구 활동을 통해 제시한 시스템공학 프로세스와 시스템안전 프로세스의 통합 프로세스 모델[4]을 바탕으로 프로세스 수행에 따른 산출되는 데이터의 입·출력물의 속성을 분석 하여 클래스 다이어그램을 제시한다. 따라서 이렇게 제시된 클래스 다이어그램을 바탕으로 프로세스의 흐름에 따른 데이터 상호 연동성 분석에 따른 제안된 통합 프로세스 모델에 충족하는 인터페이스 모델을 제안한다. 그밖에, 구축된 인터페이스 모델은 전산지원 도구를 활용해 인터페이스 모델의 구축 및 검증에 관한 연구를 수행 하였다. <Figure 4>을 통해 인터페이스 모델 구축에 대한 연구 수행 방법을 도식화 하였다.

본 연구의 영역은 <Figure 5>와 같다. 일반적으로 시스템공학에서 시스템 수명주기는 <Figure 5>에서 제시되는 것처럼 여러 형태로 제시되고 있다[1][2][7]. 이러한 여러 단계들을 아래와 같이 3가지 큰 단계로 정의 하였으며,

- Concept Development
- Engineering Design
- Post Engineering

본 연구는 개념설계 단계로 범위를 한정 및 설정 하였다.

<Table 1> A set of classes and their attributes

Class	Definition	Attribute
Hazard	관련 개념이 존재하여 발생했던 위험이나, 상위 수준에서 예상되는 위험상황	- 예상 피해 정도 - 예상 발생 빈도
Risk	위험원(Hazard)의 발생빈도 및 확률을 수치적으로 표현한 것	- 위험도 - 상태
Failure	기능의 목표달성 실패, 고장 또는 결함	- 발생확률 - 원인 - 탐지 방법
Mitigation	위험의 확률이나 결과를 줄이기 위한 노력	상태 완화 정도 영향
Risk Acceptance Criteria	설계 및 안전 활동의 허용 가능한 위험을 결정하기 위한 기준	- 정성적 기준 - 정량적 기준 발생 가능성 심각성
Parameter	설계 및 안전 활동의 기준 지표	정량적 기준 정성적 기준

3. Data Modeling

3.1 통합프로세스 모델 수행에 따른 산출 데이터 분석활동

Design Phases	Integrated Process Model _(Input & Output) Data	Integrated Data Model Class												
		System	Function	Requitements	Safety Program Plan	Constraint Req.	Safety Req.	Documents used as input to safety	Hazard	Risk	Failure	Action	Event	Parameter	Mitigation
Pre-Conceptual Design	Mission Req.	●		●											
	Prelim. System Spec.			●											
	Mission Needs Statement			●											
	Scope definition statement	●		●											
	Safety Plan Doc.				●			●							
	Identified Safety Hazards								●						
	Pre-Conceptual Hazards								●						
	Tailored Safety Design Strategy														
Conceptual Design	Prelim. Hazard Analysis Data								●	●	●	●	●	●	●
	Specified Safety Function						●								
	Specified Safety Classifications														
	Updated Safety design Plan				●										
	Conceptual Safety Validation Doc.				●										
	System High Level Unmitigated Analsis									●	●	●	●	●	●
	SEMP				●										
	Operation Req. Doc.							●							
	Constraint Conditon Doc.					●		●							
	Environment Analysys Doc.							●							
	Interface definition Doc.							●							
Preliminary Design	Detailed Hazard Analysis									●	●	●	●	●	●
	Prelim. Safety Doc.				●		●								
	Prelim. Validation Doc.														
	Intial Product Baseline Doc.		●												
	System Level Unmitigated														
	Updated Safety Fuction						●								
	Updated Safety Design Plan				●										

<Figure 9> Data linkages existing between the integrated process model and data model

<Figure 6>에서 제시되는 통합된 프로세스 모델을 기반으로 개념설계수행 시에 요구되는 안전 분석 활동과 설계활동에 따른 설계 산출물의 분석을 수행하였다. 산출 데이터 분석활동은 아래와 같이 수행하였다.

Step 1. 설계활동 및 안전 활동의 정의: 개념설계단계에서 요구되는 설계활동, 위험분석 안전활동의 정의.

Step 2. 활동에 따른 생성 산출물 정의: 설계활동 및 안전 활동에 따른 산출물의 정의.

Step 3. 생성 산출물 포함 요소 분석: 설계 및 안전 활동에 따른 생성 산출물이 포함하고 있는 요소 분석 및 코드화.

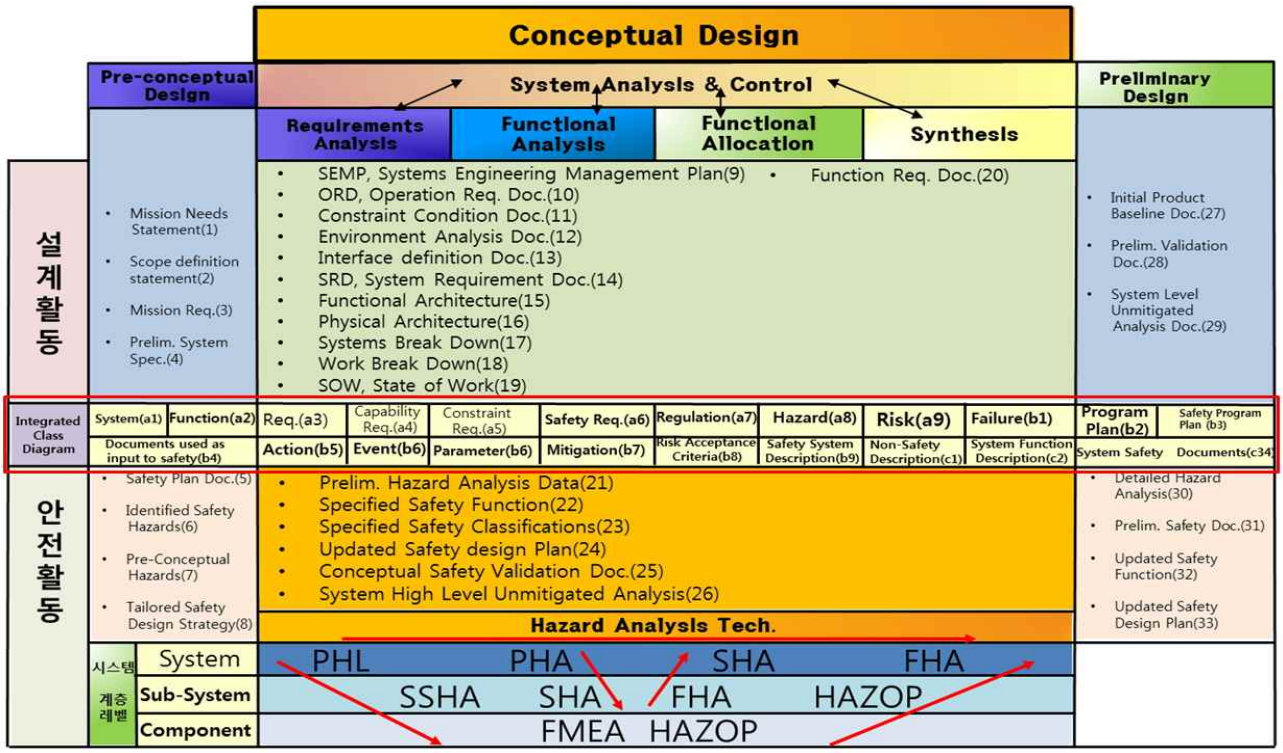
Step 4. 산출물 공통요소 분석: 활동에 따른 산출물 구조의 메트릭스를 생성하여 공통요소 분석 수행, 각 공통된 입·출력을 클래스로 정의한다.

3.2 통합프로세스 모델 수행에 따른 산출 데이터의 속성 분석

<Figure 6>에서 제시하는 통합프로세스 모델에 따른 수행 산출물을 <Figure 7>과 같이 정리하였다. 따라서 산출된 데이터 분석을 통해서, 산출물 사이의 공통된 입·출력 요소들이 많음을 발견하였다. 개별 데이터가 지니고 있는 데이터 속성 분석은 데이터를 바탕으로 개념적 모델을 생성하는데 매우 중요한 활동이다. 데이터 속성 분석을 통해, 중요한 공통 속성은 개별 클래스로 도출하고, 공통 요소가 없는 상황 또는, 중요도가 적은 상황에 대해서는 개별 클래스로 정의 또는 제거하였다. 예를 들어, <Figure 8>과 <Table 1>을 통해서, 알 수 있듯이, Risk, Hazard, Failure의 경우, Parameter라는 공통된 속성을 지니고 있다. 또한 Parameter는 시스템 설계 및 안전 활동에 있어서 매우 중요한 척도를 제공하므로 별도의 Class로 정의하여 Class간의 관계를 정립하였다.

3.3 구축된 통합 데이터 모델

3.1에 제시한 절차를 통해 <Figure 7>과 같은 수행활동과 그에 따른 산출물 분석활동을 수행하였다. 산출물이 내포하고 있는 본질인 속성을 분석하여, <Figure 8>의 상부에 주된 활동을 보이는 시스템공학 활동과 하부에 정의한 시스템 안전 활동을 통해 산출되는 데이터 들 간의 관계정의를 구축하였다. 식별된 정보들을 클래스로 정의하여 UML(Unified Modeling Language)[8]의 Class Diagram으로 표현하였다. 따라서 상위수준에서 시스템공학활동과 시스템 안전 활동의 개념적 수준의 활동을 용이하게 제시하고 있다. 추후, 제시된 모델을 기반으로 엔지니어로 하여금 설계와 안전 활동에 있어서 통찰력을 제공할 것이다. 또한, 본 자료를 바탕으로 각 분야의 전문엔지니어는 보다 상세화 시켜 진행하면 되겠다.



<Figure 10> Construction of data interface model for the integrated process based on data model classes

4. 통합 설계 환경의 구축

4.1 통합 설계 프로세스 모델과 통합 데이터 모델 입·출력물의 데이터 상호 연동성 분석

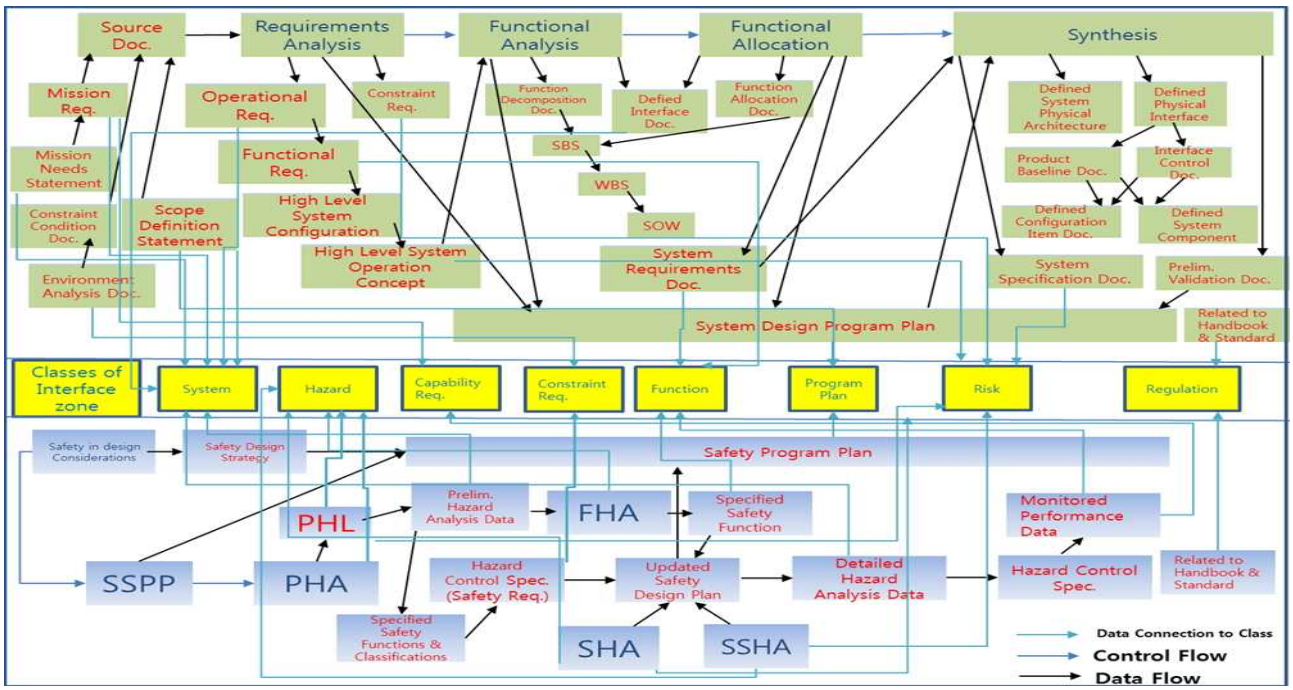
모든 존재하는 프로세스에는 입·출력물이 존재하기 마련이다. 선행연구[9]에서 제시한 <Figure 5>의 통합 프로세스 모델을 통해서 시스템 개념설계 단계, 그리고 개념설계 단계를 구성하는 서브-설계단계 및 시스템 계층 레벨에 수행해야하는 해당하는 수행 안전 활동과 산출물 정의하여 하나의 통합 수행 모델로 제시 했었다. 또한, <Figure 6>과 <Figure 7>을 통해 알 수 있듯이 이번 연구를 통해, 통합설계 프로세스에 따른 산출물과 산출물이 지닌 본질 특성인 속성을 분석하여 산출물의 개념적 관계를 통합 클래스 다이어그램을 통해 제시하였다. 본 연구단계에서는 앞의 연구 활동 결과를 바탕으로 통합프로세스 모델과 통합 데이터 모델 사이의 데이터 연동성을 분석하였다. 연동된 데이터 모델을 통해서, 총체적인 관점에서 통합프로세스 모델을 통해 수행되는 활동과 산출물이 다른 데이터들과 어떠한 연관관계를 지니고 있는지, 다시 말해, 시스템공학 설계프로세스와 시스템 안전 활동, 그리고 산출물의 개념적 데이터들 간의 관계를 한눈에 바라볼 수 있는 관점을 제시한다. 예를 들어 설명하자면, Pre-Conceptual Design 단계에서 설계특성을 지닌 Scope Definition Statement의 경우, 개발 대상 시스템의 범위를 언급하고 있기 때문에 시스템 개발의 매우 중요한 문서중 하나이다. 따라서 이러한 문서는 데이터 모델의 Class인 System과 매우 밀접한 관계를 생각할 수 있다. 또한, 안전 활동 특성을 지닌 Safety Plan Doc.의 경우, 산출물의 속성적 분석과 데이터 모델을 통한 관계분석을 통해 System Safety Documents라는 Class에 속함을 알 수 있다.

4.2 구축된 데이터 중심 인터페이스 모델

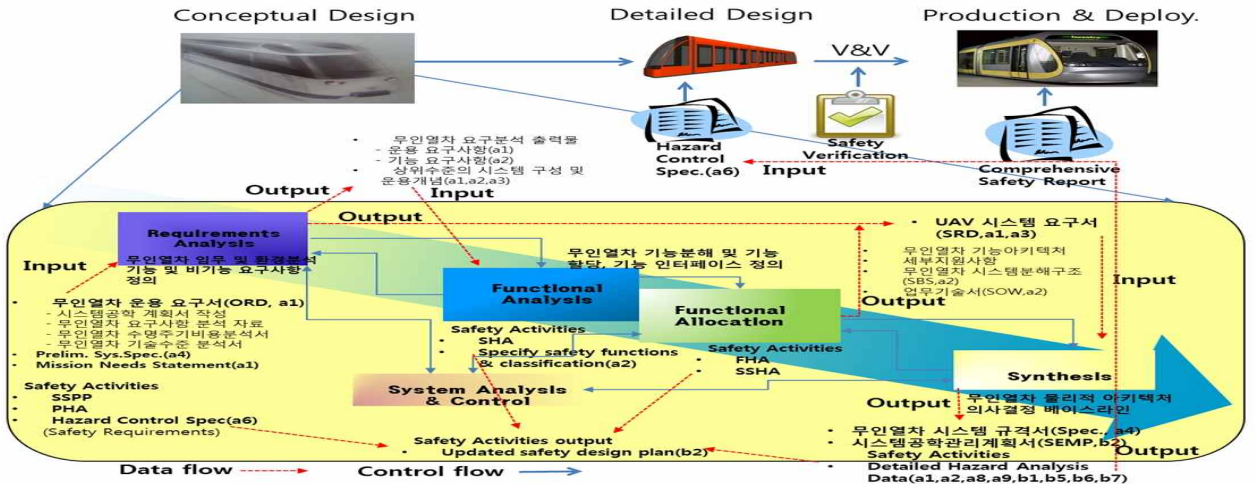
<Figure 11>을 통해 제시한 것처럼 통합 설계프로세스의 인터페이스 모델을 구축하기 위해서 시스템공학 설계 프로세스와 시스템 안전 프로세스에 대해 동일한 수명주기 기준을 가지고 개별 프로세스 분석을 통해, 활동에 따른 산출물을 분석·정리하였다. 인터페이스 모델을 구축하기 위해서 선행연구로 <Figure 8>을 통해서 제시한 것처럼 클래스 다이어그램을 통해 시스템설계 활동과 안전 활동에 따른 데이터들 사이의 관계를 정의하여 제시하였다.

<Table 2> Data linkages

설계 산출물	The Class of Class Diagram	안전 활동 산출물
Mission Req.	System(a1)	Prelim. Hazard Analysis Data
Mission Needs Statement		
Scope definition statement		Safety Plan Doc.
Operational Req. Doc.		
Interface definition Doc.		Detailed Hazard Analysis Data
Intial Product Baseline Doc.	Function(a2)	Monitored Performance Data
Mission Needs Statement		Specified Safety Function
Interface definition Doc.		Updated Safety Function
Prelim. System Spec.	Requirements(a3)	Prelim. Safety Doc.
Mission Needs Statement		
Prelim. System Spec.	Capability Req.(a4)	Monitored Performance Data
Mission Req.		
Constraint Condition Doc.	Constraint Req.(a5)	Safety Requirement
Environment Analysis Doc.		
Constraint Condition Doc.	Safety Req.(a6)	Prelim. Safety Doc.
Environment Analysis Doc.		
Operational Req. Doc.		Safety Requirement
Interface definition Doc.		
Tailored Standard	Regulation(a7)	Tailored Standard
Tailored Handbook		Tailored Handbook
System Level Unmitigated Analysis Doc.	Hazard(a8)	Identified Safety Hazards
		PHL(Preliminary Hazard List)
		Pre-Conceptual Hazards
		Prelim. Hazard Analysis Data
		Detailed Hazard Analysis
System Level Unmitigated Analysis Doc.	Risk(a9)	Prelim. Hazard Analysis Data
		Identified Safety Hazards
		Detailed Hazard Analysis
System Level Unmitigated Analysis Doc.	Failure(b1)	Prelim. Hazard Analysis Data
		Identified Safety Hazards
		Detailed Hazard Analysis
Prelim. Validation Doc.	Program Plan(b2)	Safety Plan Doc.
Intial Product Baseline Doc.		Updated Safety Design Plan
Scope definition statement		Prelim. Safety Doc.
Systems Engineering Management Plan		



<Figure 11> A representation of the interface data model in terms of data model classes.



< Figure 12 > Application of the resultant interface model in the design of a train system operated without drivers.

<Figure 9>을 통해서는 기존에 제시한 통합설계 프로세스 모델을 통한 산출물과 제시한 데이터 모델과의 연동성 분석을 바탕으로 인터페이스 모델 구축하는데 있어 활용하였다.

결과적으로 제시된 데이터 중심 인터페이스 모델을 통해서 알 수 있듯이 시스템설계활동과 안전 활동을 통한 산출물이 클래스 다이어그램의 클래스(Class)라는 공통된 매개체에 연계되어 있다는 것을 알 수 있다. 따라서 설계자, 안전 관리자 또는 프로젝트매니저와 같은 제3자가 필요로 하는 정보로부터 Class라는 매개체를 통해 관련 정보에 대해 손쉽게 파악 및 획득이 가능해 졌다. <Table 2>를 통해서 Class라는 공통 매개체 기반의 데이터 흐름을 <Figure 8>, <Figure 9>, <Figure 10>을 기반으로 정리하였다. 구축된 인터페이스 모델을 기존 제시한 통합 설계 프로세스 모델의 참고모델로서 활용해 나아간다면 개선된 설계 신뢰성을 바탕으로 보다 높은 시스템 안전성 확보가 가능해 질 것이다.

5. 구축된 통합 인터페이스 모델의 검증

5.1 무인화 열차 시스템 설계 적용 사례

최근 자치단체에서 건설하는 경전철 사업의 경우, 운행되는 열차 시스템은 기관사가 없이 열차가 스스로 자율 운행되는 무인화 시스템으로 운용되고 있다. 따라서, 기존 유인열차 시스템의 운용 때보다 체계의 구성이 보다 복잡해져 인터페이스 측면과 안전성 측면이 보다 강조되고 있다. 이러한 시스템의 특징은 제어시스템에 대한 설계 신뢰도가 시스템 운용과 설계 안전도에 큰 영향을 미친다. 따라서, 기존 유인 열차와는 다른 개념의 제어기술이 개발되어야 한다. 본 논문에서 제시하는 인터페이스 모델을 반영하여 설계활동과 안전 활동의 상호 유기적인 수행을 통해 인터페이스 측면을 보다 강화하고자 한다. 따라서, 본 논문에서 제안한 데이터 중심 인터페이스 모델을 개발 절차에 따라 무인열차 시스템에 적용 하였다.

개념설계 단계의 무인화 열차 시스템설계에 있어서 <Figure 6>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 식별하여 <Figure 12>와 같이 적시하였다.

개념설계 단계에서는 상위수준의 안전활동이 이루어진다. 따라서 대부분의 안전활동이 요구사항 분석 단계에 적용되며 이러한 과정을 거쳐 무인열차 운용 안전 요구사항, 기능 안전 요구사항 등이 도출된다. 이러한 안전 관련 요구사항을 바탕으로 안전 기능 식별과 기능 위험분석을 통해 기능할당 및 기능 인터페이스를 정의하는데 반영된다는 것을 <Figure 12>를 통해 확인할 수 있다. 요구사항 분석 단계에서 산출된 무인열차 운용 요구서와 기능 분석 및 할당 수행을 통한 산출물로 무인열차 시스템 요구서가 작성된다. 따라서, 최종적으로 개념설계 단계의 통합프로세스는 무인열차 시스템 요구서를 바탕으로 최종적 시스템 규격서(Spec.)를 생성하게 된다. 이러한 설계 및 안전 활동을 통한 산출물을 클래스 다이어그램을 통해 분석하여 매칭되는 클래스를 산출물에 표기함으로써 설계활동과 안전 활동의 데이터 사이에 상호유기적인 관계로 진화할 수 있다.

6. 결론 및 요약

오늘날 대형 복합 시스템 개발 및 운용단계에서 문제되는 것의 핵심 이슈는 인터페이스 측면이다. 특히, 본 논문에서는 기존에 제시한 대형복합 안전중시 시스템 개발 사업에 있어 활용 가능한 시스템공학 설계프로세스와 시스템안전 프로세스의 통합 프로세스 모델을 활용하였다. 따라서 통합설계 프로세스 모델을 통한 설계활동과 안전활동 수행을 통해 생성되는 산출물들이 지닌 속성을 분석하여 클래스 다이어그램으로 관계를 정의해 표현하였다. 따라서 설계활동과 안전 활동의 수행에 있어서 Class라는 인터페이스 매개체를 제시하였다. 이러한 인터페이스 매개체를 기반으로 설계 산출물과 안전 활동을 통한 산출물 간의 상호연동성 분석이 가능해졌다. 따라서 생성된 데이터 중심 인터페이스 모델을 통해, 설계를 수행하는 엔지니어와 안전관리 엔지니어 사이, 프로젝트 매니저로 하여금 공통의 사고를 바탕으로 보다 체계적으로 설계수행을 통해 보다 개선된 설계 신뢰도를 갖춰 대형복합 안전중시 시스템의 안전성을 확보할 수 있을 것이다. 따라서 기존에 제시한 통합설계프로세스 모델을 바탕으로 설계 및 안전 활동의 수행을 통해서 이번에 제안한 데이터 중심 인터페이스 모델을 참조 모델로 활용한다면 상위 수준에서의 보다 개선된 시스템 설계 활동 및 안전 활동을 동시에 고려한 설계 활동이 가능해짐에 따라 안전중시 시스템의 개발 사업관리 측면의 활용적 가치에 기여하였다고 생각 한다. 후속 연구 활동 또한 활발히 진행되었으면 한다. 추후 연구에서는 연구범위를 확장시켜 안전중시 시스템 설계에서 보다 개선된 인터페이스 모델을 제시하는 연구가 필요할 것이다.

7. 참 고 문 헌

[1] A. Kossiakoff and W. N. Sweet, SystemsEngineering Principles and Practice. New Jersey: Wiley, pp. 117-138, (2003). [2] A. E. Clifton, “Hazard analysis techniques for system safety.”, Hoboken, New Jersey: John Wiley & Sons, Inc., (2005)

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

[4] 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)

[5] 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. 438-443, (2007)

[6] J. H. Yoon and J. C. Lee, “A Study on Integrated SE Process for the Development of the Railway Systems with Safety Assessment Included,” Korean Society for Rail, vol. 11, pp. 19-26, (2009)

[7] Systems Engineering -System life cycle process, in ISO/IEC 15288:2002(E): International Organization for Standardization, (2002)

[8] UML (Unified Modeling Language) 2.4, Omg.org Retrieved, (2011)

[9] 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)

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