Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 10 pp. 68-78, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.10.68
ISSN 1975-4701 / eISSN 2288-4688

FMEA 안전분석 기법을 활용한 차상중심 열차제어시스템의 아키텍처 무결성 향상을 위한 검증 방법론 구축에 관한 연구

김주욱[1], 오세찬[1], 김금비[1], 심상현[2], 김영민[2*]
[1]한국철도기술연구원, [2]에스피아이디

On the Improving Integrity for Verification method of Train-Centric Train Control System Architecture using FMEA Safety Activity

Joo-Uk Kim[1], Seh Chan Oh[1], Keum Bee Kim[1], Sang-Hyun Sim[2], Young-Min Kim[2*]
[1]Korea Railroad Research Institute, [2]SPID Co, Ltd.

요 약 최근 철도 열차제어시스템은 최첨단 기술로 인한 무선통신기반 개발의 수요와 이에 따른 환경의 다변화로 인해 안전에 대한 쟁점도 증가하고 있다. 이에 따라 기존의 열차제어시스템에서 다루는 지상 설비 설계에 대한 단계별 안전 활동 강화의 필요성 역시 강조되고 있다. 국내 철도 산업은 대다수 열약한 산업환경으로 구성되어 있다. 이러다 보니, 설계 산출물에 대한 생성에 초점이 맞춰져 있지, 산출물에 대한 검증 방안 및 적용에 대한 역량이 상당히 부족한 실정이다. 따라서, 본 논문에서는 열차제어시스템 설계 단계의 아키텍처 산출물 검증 방안을 확보하기 위해 안전분석 산출물을 바탕으로 확보 가능한 방법에 대해 기술하고 있다. 이렇듯 설계적 산출물에 대한 검증방안을 구축하고 직접 수행에 따른 설계적 무결성을 높이고자 한다. 특히, FMEA 안전 분석 기법을 활용해, 안전 분석 기법을 통해 개별 단계별 산출물의 활용을 통한 아키텍처 산출물과의 연계성 확보를 통해 무결성 확보를 위한 기술적 접근법을 기술하였다. 본 연구의 결과를 토대로 안전성 향상 접근에 대한 시험 활동 재정립을 통해 개선함으로써 향후 모델 기반 열차제어시스템 개발 시 개념설계에서 발생할 수 있는 안전성 이슈를 제거 함에 따라, 설계적 비용 및 시간을 절감 및 안전성 향상을 기대할 수 있을 것으로 기대된다.

Abstract Safety is the most important factor for train control systems. Model-based design and safety activities for way-side equipment in train control systems are important factors. Model-based architecture verification was carried out to develop an effective control system, which is represented by model-based failure mode and effects analysis (FMEA). An architecture verification method was created based on FMEA to take advantage of a design model and improve the train safety control system. Case studies were applied to architecture verification scenarios, and the results demonstrate the usability of the method. The improved method is expected to reduce the cost and time in the conceptual design for future development of model-based verification train control systems.

Keywords : Train-Centric Train Control System, Systems Engineering, Railway System, Safety Critical System, Failure Mode & Effects Analysis

1. 서론

국내 상당수 도메인 분야의 안전 및 설계 활동이 별개의 활동으로 진행 중에 있다. 이러다 보니, 상당수 안전 요구사항의 발견 및 설계적 반영에 대한 결과물로 반영되어야 할 사항들이 오늘날 대형화/복잡화 특성의 시스템 개발시 상당한 어려움을 겪고 있다. 상당수 안전활동 및 시스템 설계 활동들이 시스템 설계 초기 활동인 개념

본 연구는 한국철도기술연구원 주요사업의 연구비 지원으로 수행되었습니다.
*Corresponding Author : Younge-Min Kim(SPID)
Tel: +82-2-3453-5345 email: ymkim@spidconsulting.com
Received September 27, 2016 Revised October 6, 2016
Accepted October 7, 2016 Published October 31, 2016

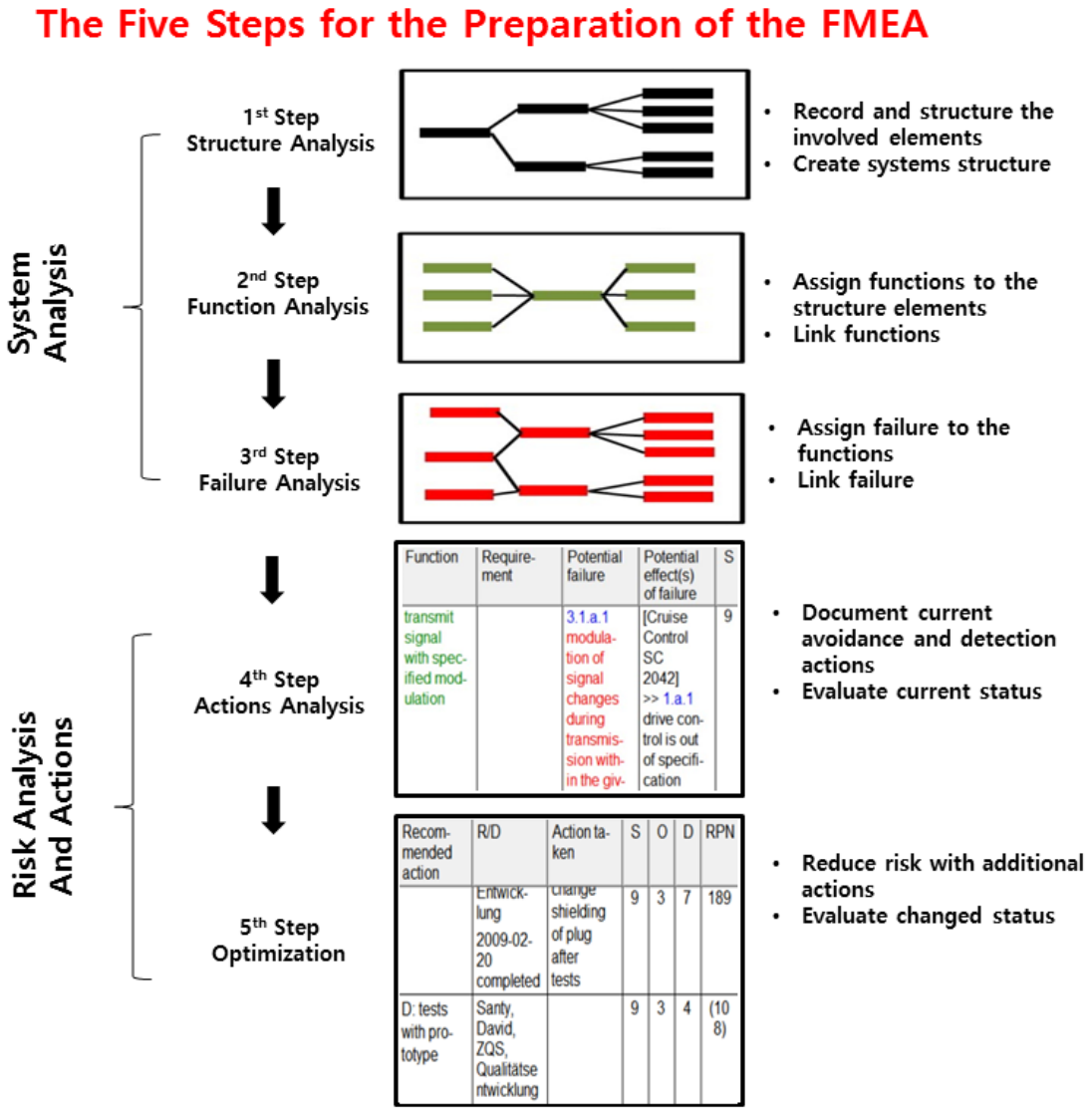

Fig. 1. The Five Steps for the Preparation of the FMEA[1].

설계 단계가 아닌 상세설계 단계에 집중되어 활동주이기 때문이다. 이러다보니, 신규 컨셉을 기반으로 개발되는 시스템 체계의 경우 물리적 구조를 제대로 반영하지 못하는 측면이 존재하고 있고 그 결과 안전활동의 수행에 있어서도 제약적인 산출물만을 제공하고 있다. 이러한 결과, 시스템의 상위수준에서 안전/설계적 측면의 활동이 강조되고 있는 시점에 와있다.

본 연구진은 국내에서 아직 개발되지 않은 열차제어시스템을 개발 중에 있으며, 이로 인해 발생될 수 있는 설계적 문제를 사전에 해결하고 이를 바탕으로 안전성 확보를 위해 본 연구를 수행하였다. 본 연구에서 대상으로 여기는 열차제어시스템은 선로의 신호, 운전, 역(Station) 등의 정보를 기관사에게 제공하고, 선행열차와의 간격 제어와 더불어 제한속도 초과 시 열차의 안전을 확보하는 기능을 담당하고 있다[1]. 특히, 열차제어를 위한 신호방식으로 기존의 자동열차정지(ATS: Automatic Train Stop) 방식으로부터 고속, 고밀도 운행에 대비한 자동열차방호(ATP: Automatic Train Protection) 방식이

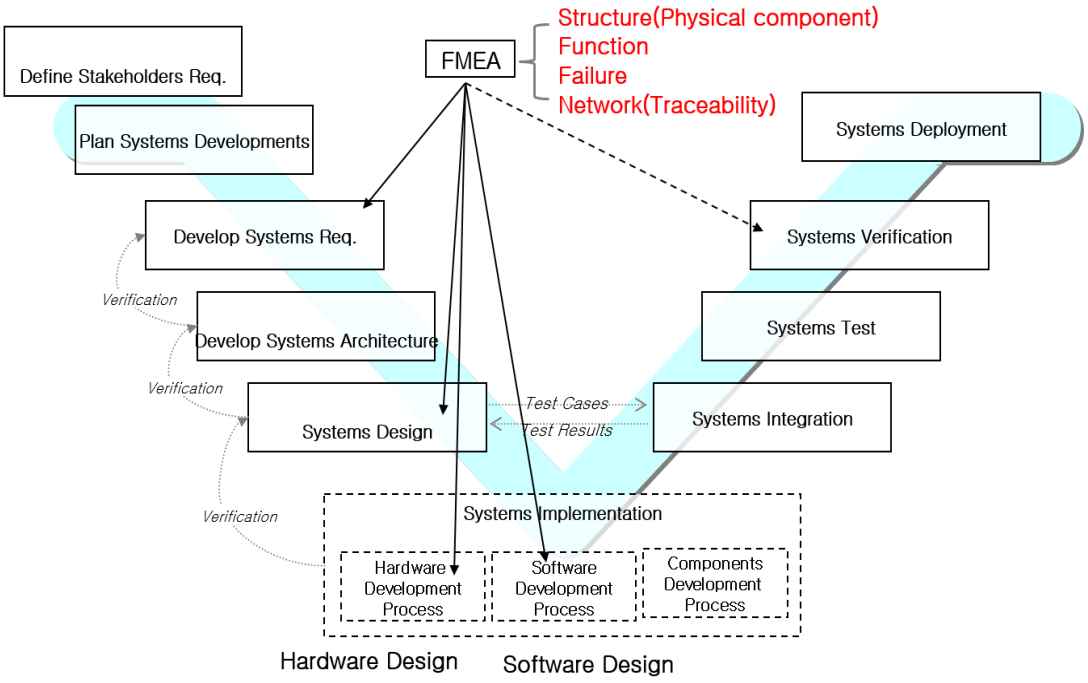

Fig. 2. FMEA Perspective of the Vee Model

존재하고 있다[2].

최근 철도산업의 발전된 기술로 인해, 열차의 고속화 또는 무인화에 이르기 까지 다양한 열차들이 노선에서 운용되고 있는 실정이다. 이러한 다양한 노선에서 운행되고 있는 차량들이 기하급수적으로 늘어남에 따라, 최근 열차제어에 관여하는 신호시스템의 중요성에 대해서 상당수 인지하고 설계적 신뢰성을 높여 안전성 확보를 위해 본 연구를 수행하였다. 기존의 열차제어 신호시스템은 Fig. 4의 좌측과 같이, 지상에서 관제하여 열차의 운행을 통제하곤 하였지만, 오늘날 열차의 고속화 및 기하급수적으로 늘어나는 신호제어의 중요성이 이슈되고 있다. 기존의 열차제어 시스템의 운용개념은 위험발생 시 ATS가 지상에서 제한속도를 생성하여 기관사 실수에 대한 열차보호만을 담당하는 반면, ATP는 열차운행에 필요한 각종 정보를 지상 설비를 통해 차량으로 전송하고, 차량의 컴퓨터를 통해 속도프로파일의 생성 및 열차방호를 수행하였다. 본 연구에서는 Fig. 4의 우측 그림과 같이, 차상, 다시 말해, 차량에 ATP 신호체계를 탑재하여 차량 간 신호시스템을 제어 가능하도록 설계하고 있다. 이렇다 보니, 기존에 존재하지 않은 새로운 운용개념으로부터, 시나리오가 발생되고, 그것을 구현하기 위한 물리적 구성 또한, 달라지고 있다. 국내와 같이, 설계/안전 영역에서 개념설계 영역이 취약한 상황에서 새로운 개념을 바탕으로 생성된 아키텍처 산출물에 대한 검증 방안이 시급한 실정이다.

따라서, 본 연구에서는 차상중심 열차신호제어시스템이라는 신규 신호제어 시스템을 대상으로 생성된 설계 산출물인 아키텍처 산출물에 대한 무결성을 높이고자 FMEA(Failure Mode Effects Analysis) 안전분석 기법을 활용해 본 연구를 수행하였다.

관련된 연구로는 최근 자동차 도메인 분야에서 설계적 신뢰성을 바탕으로 차량의 안전성을 확보하기 위해 ISO 26262[4]라는 국제 표준이 유럽을 중심으로 등장하였다. 해당 표준에서는 설계적 문제의 사전 식별을 Fig. 1과 같이, FMEA 안전분석 기법을 기반으로 요구하고 있다. 해당 안전 분석 기법은 크게 5단계의 접근을 기반으로 시스템을 분석하고 위험사항을 평가하고 조치하는 과정으로 구성되어 있다. 특히, FMEA 기법은 본 연구의 대상인 아키텍처 산출 과정과 상당한 밀접한 정보를 제공하기 때문에 본 연구에서는 연계성 확보를 위해 노력하였다.

추가적인 관련 연구로는, Ward(2011), Grello(2011)

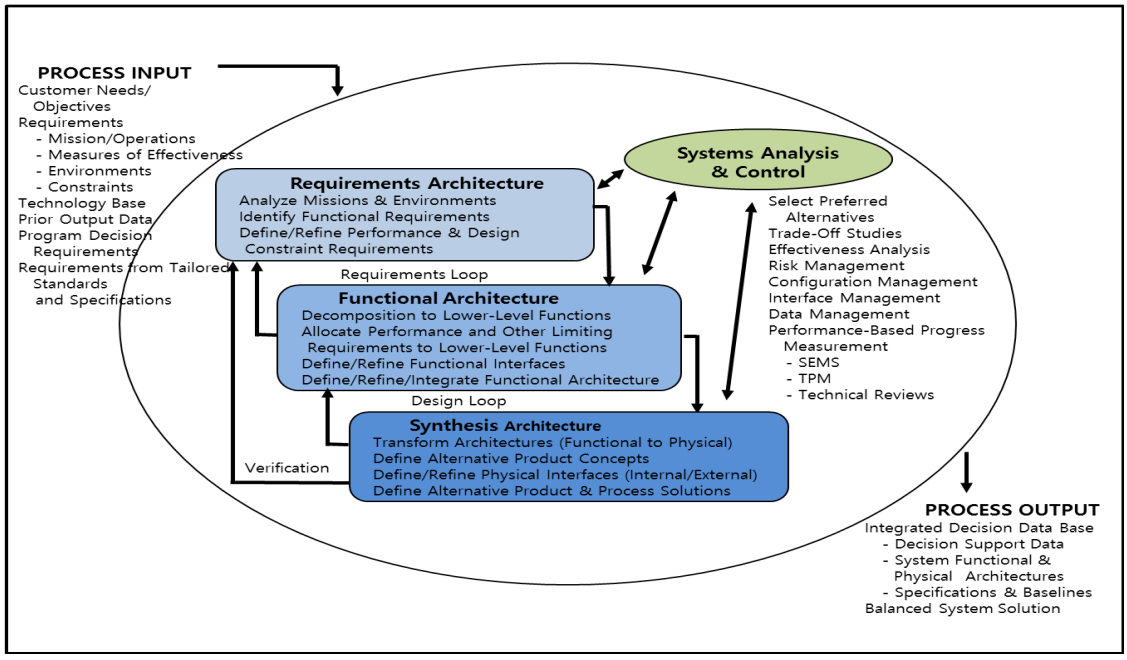

Fig. 3. Systems Architecture Process for general systems design[9].

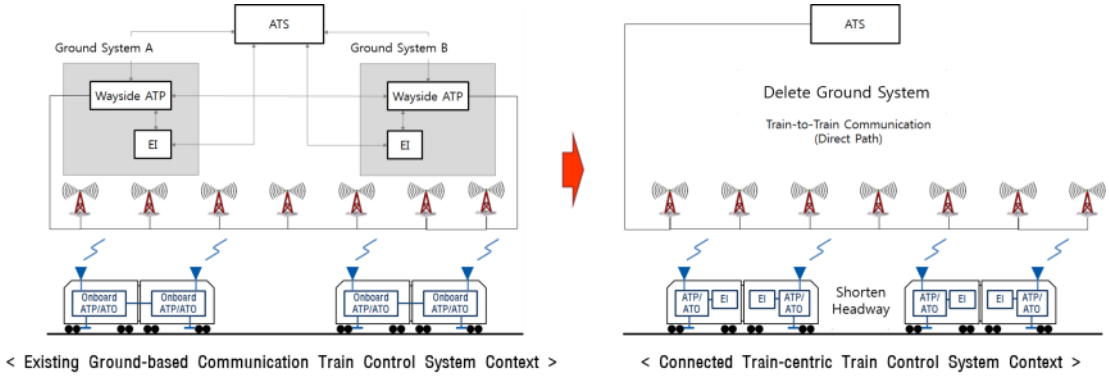

Fig. 4. Train-centric Train Control System

는 오늘날 시스템의 대형화로 인해 발생될 수 있는 안전 문제들을 사전에 식별하고 이를 통해 설계적 대응을 수행하기 위해서 다양한 운용 시나리오를 생성함에 있어서 Model-based Systems Engineering 접근을 활용하여 시스템 구축 및 인터페이스 정보 식별 등에 대한 체계적 접근을 하는 것을 알 수 있다[5][6]. 이러한 점은 본 연구의 안전분석 기법을 통해 기능오류의 다양한 모드가 분석된다는 측면에서 상호 활용적 가능성을 높이는 대목이 된다.

또한, 본 연구의 방법론과 밀접한 연구인, 설계와 안전성 측면의 상호 고려를 통한 검증 수행에 관한 연구를 고찰하였다. Prabhu 외(2014), Keith 외(2014)는 시스템 설계 변경에 따른 다양한 구성요소들의 오류 및 정보를 확인하기 위한 절차를 개발하고 VV&T(Verification, Validation & Test) 수행 시 상호간의 인터페이스를 빠르게 식별할 수 있도록 모델 기반 접근을 활용하여 접근하였다[7][8]. 하지만 이러한 검증절차는 신규 시스템의 개발시, 검증에 필요한 근원적 데이터가 상당히 결여 되

어 있다. 이러한 측면에서 본 연구에서는 안전분석 기법의 수행을 통한 산출물을 바탕으로 검증과정에 필요한 근원적 정보를 제공한다는 측면에서 차이점을 지니고 있다. 따라서, 본 연구에서는 안전분석 기법와 설계적 기법 간의 연동성 파악을 바탕으로 차상중심 열차제어시스템 아키텍처 산출물의 검증 가능한 프로세스 모델을 만들고자 연구하였다.

본 논문의 구성은 다음과 같다. 서론에서는 본 연구의 사회, 기술 및 연구 동향을 기술하였고, 2장에서는 차상중심 열차제어시스템 FMEA 안전성 활동을 기반한 시스템 아키텍처 산출물의 검증 연계방안에 관한 필요성을 제시하였다. 3장에서는 FMEA 안전분석과 아키텍처 산출물 생성을 위한 단계별 활동 및 산출물이 지니고 있는 속성 정보를 분석하였다. 분석된 결과를 바탕으로 연동성 제안을 통해, 아키텍처 산출물 검증에 관해 연계 수행 가능한 방법론을 정립하였다. 4장에서는 차상중심 열차제어시스템을 대상으로 적용 사례를 제시하여 제시된 절차를 검증 확립하였다. 마지막으로 5장에서는 본 논문의 결과 정리 및 공헌에 대해 기술하였다.

2. 문제의 정의

2.1 안전분석 결과를 반영한 시스템 안전요구사항 생성 및 아키텍처 반영의 필요성

시스템 레벨에서의 설계 단계에서 요구되는 안전 활동에는 다양한 안전관리 기법이 요구되고 있다. 특히, 대표적으로 철도 분야에서 활용되는 안전 분석 기번은 SHA(System Hazard Analysis), SSHA(Sub-system Hazard analysis), FMEA(Failure Mode Effects Analysis), FTA(Fault Tree Analysis) 기법이 있다. 특히, Fig. 2와 같이, FMEA 안전분석 기법은 시스템 수준의 아키텍처 산출물과 연계성을 확보하는데 있어서 가장 적합한 안전분석 기법이라고 볼 수 있다. 이러한 이유는 시스템 아키텍처 산출물은 시스템 수준에서의 구조적 산출물(구성품 식별) 및 거동적 산출물(기능 식별)을 기반으로 종합된 하나의 산출물이기 때문이다. 특히, FMEA 안전활동 또한 구조적, 기능적 산출물을 기반으로 안전 분석이 수행되기 때문이다. 이러한 맥락에서 FMEA 안전분석 활동 기반 산출물과 아키텍처 산출물의 연계성 확보가 필요하다는 것을 알 수 있다.

2.2 FMEA 안전성 활동/산출물을 통한 차상중심 열차제어시스템 아키텍처 무결성 검증의 필요성

국내 열차 시스템 설계 활동과 안전활동의 체계 적인 프로세스 아래 상호 연동성 측면은 상당한 결여가 되어 있다. 따라서, 기존 개발 시스템이 아닌 완전한 신규 개념의 시스템 개발시 요구되는 신규 물리적 구성에 대해서 체계화된 규정하는데 상당한 어려움을 겪고 있다. 따라서, 기존 시스템이 아닌 신규 컨셉을 기반한 새로운 시스템을 개발시에 파생되는 아키텍처 산출물에 대한 검증 체계가 보다 현실적으로 필요한 시점이다. 이렇듯, Fig. 3에서 제시하는 바와 같은, 설계 산출물의 핵심 산출물인 시스템 수준에서의 아키텍처 산출물을 검증할 수 있다면 시스템 개발 초기 단계에 안전성 확보 및 설계 변경비용 절감 등 다양한 측면에서 이점을 기대할 수 있을 것이다.

2.3 설계 가변성을 고려한 안전 및 설계 활동의 필요성

오늘날 한국철도 산업은 기술력 증대로 인해, 해외 많은 국가에 철도 차량 및 제반시설과 관련해 수출하고 있는 실정이다. 이러한 다양한 국가에서 요구하는 요구사항과 해당 국가만의 법제적 기준에 따라 요구되는 사항들이 다르기 마련이다. 따라서, 개별 국가별로 요구하는 사항별로 쉽게 대응하기 위해서는 주요 가변 요소를 식별하고 그에 따른 아키텍처 설계를 구성해야 한다. 이렇게 가변 요소를 식별하고 그에 따른 아키텍처 설계 산출물을 구축한다면 설계 변경에 대한 상당한 자유로움을 가져다 갖출 수 있게 되고 보다 안전성 확보에 체계화된 접근을 수행 할 수 있게 된다. 특히, 가변 요소 식별과정에는 FMEA 안전 분석 활동을 통해서 물리적 구성품의 구조와 해당 구조(Structure)의 오류에 대한 영향을 추적 확립하기 때문에 설계적 가변 요소를 식별하고 해당 영향성 분석이 가능하다는 점에서 활용적 측면에서 적합한 안전분석 기법이 될 수 있을 것이다.

3. 안전분석 결과를 기반한 열차제어 시스템 아키텍처 검증 방법론 구축

3.1 안전활동과 아키텍처 산출물의 연계성 확보를 통한 검증 프로세스 모델 구축 방안

Table 1. The Main objectives and features of FMEA Safety Activity.

FMEA Activity	Major Purpose
Structure Analysis	Overview of the inspected product. Reuse of modules Classification and interface ,description. Establish responsibilities.
Function Analysis	Overview of the functionality of the product. Overview of the cause-effect relationships. Verification against the customer requirements. Basis for the failure analysis.
Function Failure Analysis	Identification of the possible failures) assigned to system structure and to functions. Links of the failures to the failure structures. Basis for the illustration of failures in a form and/or the preparation of the form.
Failure Effects Analysis	Assigning the existing and/or already established actions to the failures. Risk evaluation.
Failure Priority Analysis	Assigning the existing and/or already established actions to the failures. Risk evaluation.
Design Reflect (Optimization)	Identification of the actions necessary for improvement. Assessment of the risk. Checking the effectiveness of the implemented actions. Documenting the implemented actions.

본 연구의 시스템 수준 아키텍처 산출물의 안전활동 산출물 기반의 검증 방법론 모델은 차상중심 열차제어시스템의 FMEA(Failure Mode Effects Analysis) 안전분석 활동을 중심으로 시스템 수준의 아키텍처 산출물에 초점을 맞추어 검증 프로세스 모델을 구축하였다. FMEA 안전분석 기법을 기반으로 아키텍처 산출물의 검증 프로세스 모델을 갖추기 위해서는 FMEA가 지니고 있는 활동과 수행에 따른 산출물의 특성에 대한 분석이 필요하다. 또한, 설계적 관점인 시스템 아키텍처 산출물을 생성하기 위한 전제 활동 및 산출물의 속성을 분석하여 안전기법과 설계적 기법간의 연동성 확인을 통해 검증 프로세스 모델 구축에 관해 접근하였다. 따라서, 차상중시 열차제어 시스템의 아키텍처 산출물의 검증 프로세스를 구축하기 위한 과정을 다음과 같이 제시 하고자 한다.

Step 1. FMEA 안전분석 기법/시스템 아키텍처 산출물을 산출하기 위한 세부 단계를 정의 한다.

해당 단계는 시스템 설계적 측면 활동, 즉, 시스템 아키텍처 활동 및 산출물과의 연동성을 분석하기 위해서 수행해야하는 활동이다.

Step 2. 앞서 수행된 FMEA 안전분석, 시스템 아키텍처 산출물을 생성하기 위한 활동/산출물에 대한 속성을 분석한다.

Step 3. FMEA 기법 수행을 통한 구조/기능분석, 영향 분석을 통해 설계적 가변 요소를 식별한다.

Step 4, Step 1~3의 활동을 통해서 수행된 활동을 중심으로 상호 연동성 분석을 통해 연동 기반의 검증 프로세스 모델을 확립한다.

3.2 안전활동과 아키텍처 활동 및 산출물의 속성 기반 상호연동성 분석

위 3.1절에서 제시한 FMEA 안전분석 기법과 설계적 측면인 시스템 아키텍처 산출물에 대한 활동 및 산출물을 정의 하였고, 그 다음은 개별 활동 및 산출물이 지니고 있는 속성을 정의 하였다.

FMEA 안전분석 기법과 관련한 세부 단계별 활동에 관한 정의는 다음과 같다. FMEA 안전분석 기법의 수행 활동은 Table 1에서 제시되는 바와 같이, 크게 다음과 같은 단계로 구성된다.

1) 구조분석(물리적 구성품 식별)
2) 기능분석(기능 식별)
3) 기능적 오류분석(기능 오류시 발생되는 기능적 오류 식별)
4) 오류에 따른 영향분석(오류 발생시 미치는 여향 분석)
5) 오류 영향별 중요도 평가(오류 영향에 따른 심각도 분석 및 평가)

Table 2. Attributes Analysis between FMEA Safety and Architecture Activity.

FMEA Activity	Attribute	Mapping	Architecture Activity	Attribute
Structure Analysis	Component	<->	Requirements Architecture	Requirement, Function. Component, Traceability
			Physical Architecture	Component
Function Analysis	Function	<->	Function Architecture	Function, Relation
Function Failure Analysis	Function, Failure			
Failure Effects Analysis	Failure			
Failure Priority Analysis	Priority, Design Alternative	<->	Design Synthesis Architecture	Component, allocation
Design Reflect	Re-design			
	Traceability			
	Design Alternative			

6) 설계적 반영(위험도 평가에 따른 설계적 대응) 순으로 FMEA 안전분석 기법은 수행된다.

차상중심 열차제어시스템의 시스템 아키텍처 산출물을 산출하기위한 활동은 다음과 같은 순으로 요구되고 있다.

1) 요구사항 아키텍처(요구사항간 구조적/추적 관계 확립)
2) 기능 아키텍처(기능간 구조적/추적 관계 확립)
3) 물리적 아키텍처(물리적 구성품 관점에서 구조적 관계 확립)
4) 설계적 조합 아키텍처(요구사항/기능/물리적 구조를 종합적 관점에서 관계적 구조 확립) 수행 순으로 아키텍처 활동이 수행된다.

3.3 속성기반의 안전활동 및 아키텍처 연동성 확립을 통한 아키텍처 검증프로세스 모델 구축

앞선 3.2 절의 활동을 통해, 분석된 활동을 바탕으로 FMEA 안전 수행활동과 아키텍처 수행 활동의 단계별 수행내용을 분석하였다. 분석된 활동을 바탕으로 다음은 분석된 활동이 지닌 속성적 관점에서 재분석을 통해 상호 연동성 확립을 위한 근거의 자료를 Table 2과 같이 분석하였다. Table 2를 살펴보면, 좌측에는 안전기법의 활동과 우측에는 차상중심 열차제어시스템 아키텍처를 구성하는데 있어서 필요로 하는 활동과 그 개별 활동이 지니고 있는 속성적 정보를 바탕으로 상호 연동 정보가 있는 사항에 대해서 맵핑한 모습을 볼 수 있다. 이 단계에서의 특이성은 시스템 아키텍처 이행 단계에서 물리적 아키텍처(Physical Architecture)에 대한 근거를 FMEA Safety Activity 단계의 Structure Analysis 단계와 밀접한 관계가 있음을 알 수 있다. 따라서, 이러한 근거적 정보를 바탕으로 아키텍처 산출물을 구성하는 구성품이 지녀할 정보를 올바로 제공하고 있는지에 대한 검증(Verification) 활동을 수행 할 수 있게 된다.

특히, FMEA 안전분석 기법은 해당 물리적 구성품이 지닌 기능분석과 해당 기능이 지닌 다양한 상태적 변화를 통해 유발할 수 있는 Failure Effects를 분석하게 된다. 이를 근거로, 기능 아키텍처 관점에서 기능간 구조도 또는 개별 구성품(물리적 구성품)이 지녀할 기능에 대한 분석이 가능하다. 이러한 FMEA의 기능관련 산출물을 바탕으로 기능적 정보에 대한 검증 수행이 가능해진다. 하나의 기능으로부터 다양한 관점(구조적/기능적) 관점에서 추적성에 따른 영향성 분석이 가능한 정보를 제공함에 따라 아키텍처 산출물이 지닌 가변요소에 대한 분석과 검증 가능한 정보를 제공하게 된다. 따라서, 앞선 활동들을 통해, Fig. 5와 같이, FMEA 안전분석 기법을 기반으로 차상중심 아키텍처 검증 수행을 위한 프로세스 모델을 제시 하였다. 설계적 관점에서의 물리적 통합 단계에서는 앞선 설계 산출물인 물리적 구성품 식별 및 해당 구성품이 지닌 기능식별 정보를 바탕으로 아키텍처 산출물이 발생되었다면, FMEA 수행의 설계적 최적화 수행 단계 산출물의 활용을 통해, 물리적 통합 단계에서

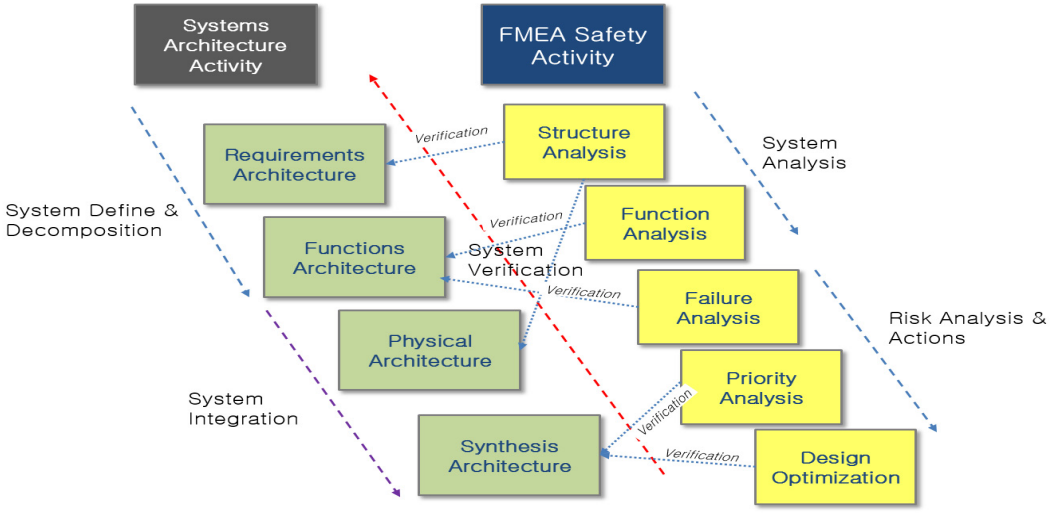

Fig. 5. Proposed integration process model for Architecture Verification.

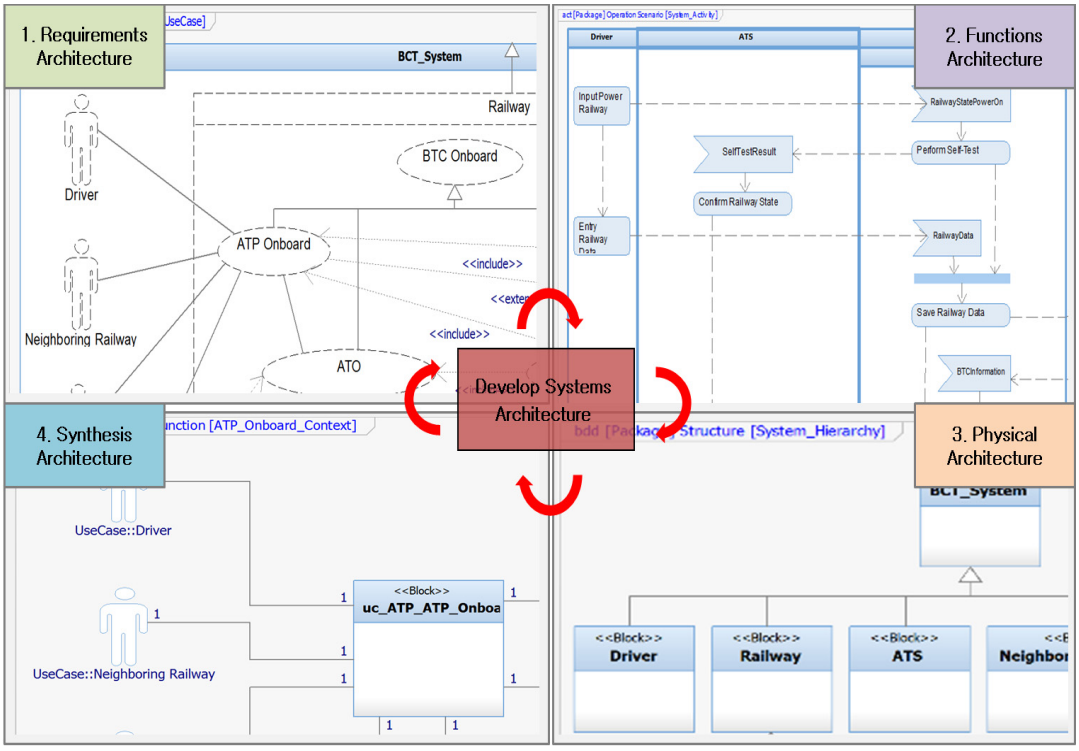

Fig. 6. Major Steps for create Architecture Artifact

어떠한 요소가 보다 재검토 되어야 하는지에 대해 검토할 수 있는 입력 자료로 활용될 수 있다. 따라서, 본 연구를 통해, 설계 단계별 산출물에 대한 검증수행의 입력 자료로서 FMEA 산출물의 연계적 정보를 제공함에 따라, FMEA 산출물 기반의 아키텍처 검증프로세스 모델을 구축할 수 있었다.

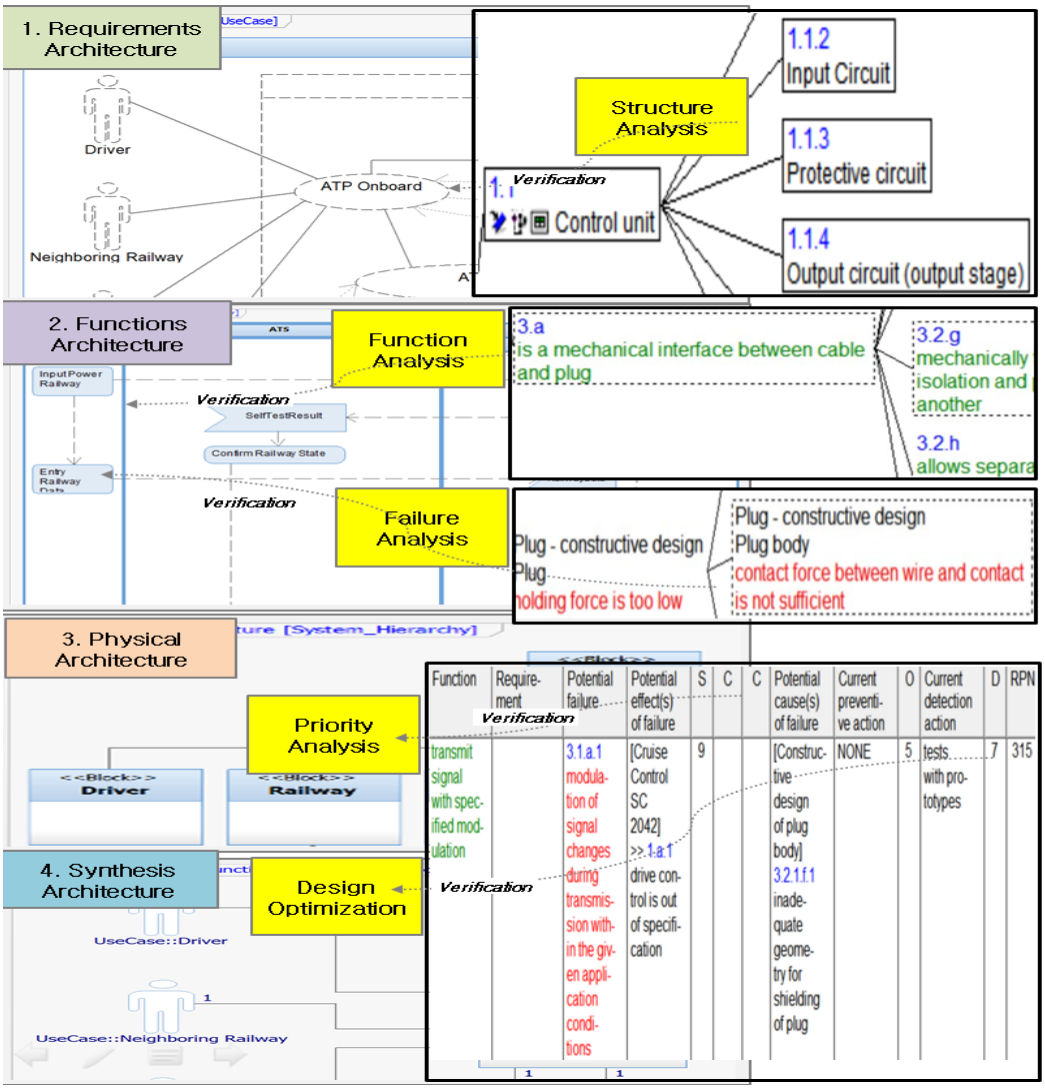

Fig. 7. Verification Activities of Train Centric Train control Systems Architecture based FMEA.

4. FMEA 안전활동 기반 아키텍처 설계 산출물의 검증 활동 수행 사례

4.1 구축된 안전/설계 산출물 연계 기반 검증 활동 수행

시스템의 최상위 수준인 시스템 레벨에서의 아키텍처 설계 산출물은 Fig. 6의 산출물과 같이 기존에 얻을 수 있었다. 기존의 차상중심 열차제어 시스템 아키텍처 산출물은 Fig. 6의 System Requirements를 기반으로 수행했었다. 예를 들어, 차상 중심 열차제어 시스템의 시스템 요구사항은 기존(기존의 무선통신기반 열차제어시스템은 열차의 위치를 궤도회로가 아닌 무선통신을 이용해 수신하고 열차의 목적지, 속도, 방향 등을 전송하여 열차를 통제한다.)의 지상에서 관제하던 열차 신호를 제어하는 개념과 달라, 지상-차상간의 양방향 무선통신의 개념이 아니다.

따라서, 아키텍처 산출물의 검증의 출발은 “차상에서 무인운전을 위한 차상설비 감시와 제어가 가능해야한다”라는 요구사항으로부터 검증 요구사항이 생성되어 출발한다. 기존의 방법으로는 Top-down 방식으로 하향

식 관련 요구사항들이 식별됨에 따라, 구조간의 영향, 또는 차상 설비의 다양한 기능으로부터 발생되는 영향에 대한 사전정보를 바탕으로 아키텍처 검증을 수행하기 제한적 접근법 이였다. 차상중심 열차제어시스템은 기존의 무선통신기반 열차제어시스템에서 차지하는 지상설비를 제거하여 차상간의 양방향 무선통신으로 구축"하였다. Fig. 5의 수립된 통합 프로세스 모델을 따라, FMEA 안전분석 기법 기반의 Fig. 6의 아키텍처 산출물을 검증할 수 있었다.

4.2 차상중심 열차제어시스템 적용을 통한 아키텍처 검증활동 수행사례

Fig. 7을 통해서, 알 수 있듯이, 개별 FMEA 안전분석 기법을 구성하는 단계의 수행결과를 따라, 아키텍처 단계별 설계 산출물에 대한 검증 과정을 수행하는 것을 볼 수 있다. 안전 분석 활동의 개별 단계에서 식별된 정보는 개별 하나가 검증활동의 근거 문장으로 활용된다. Failure Analysis의 경우, 구성품(Components)로부터 발생될 수 있는 각가지 오류 모드 분석에 대한 다양한 분기점 모습을 볼 수 있다. 분기점은 아키텍처 가변 요소와 해당 가변요소의 검증을 수행하는데 있어서 중요한 검증 요구사항 생성의 근원이 되는 자료가 될 수 있다. 또한, 기능에 대한 오류 및 다양한 영향도 분석에 따라 해당 오류의 Priority 분석을 수행하고 최종적으로 설계 최적화를 수행하게 된다. 수행된 결과를 통해, 차상중심 열차제어 시스템의 아키텍처 산출물의 검증과 검증의 결과를 바탕으로 오류를 개정해 아키텍처 산출물을 수정할 수 있는 근거를 제공할 수 있게 되었다.

5. 결론

본 연구는 FMEA 안전분석 기법을 기반으로 아키텍처 산출물의 검증 활동을 지원하기 위한 방법론을 제시하였다. 본 연구에서 제안한 방법론은 차장 중심 열차제어시스템과 같이, 새로운 개념을 기반으로 설계 되는 아키텍처 산출물에 대한 검증활동의 적용 가능한 활동을 수행하였다. 기존의 아키텍처 산출물을 검증하는데 있어서 근거적 정보는 이전 단계에서 정의된 요구사항을 기반으로 수행되어져 왔다. 하지만, 오늘날과 같은, 대형 복합 시스템 차원에서는 다양한 기능들이 탑재되고 탑재된 기능의 오류로부터 다양한 오류양향에 대한 정보는 아키텍처 산출물의 생성 및 검증에 상당한 중요 지표로 활용될 수 있는 측면이 있다. 본 연구를 통해, 또한, 차상중심의 열차제어시스템과 같은 신규 시스템 개발시에는 보다 강화된 설계 신뢰성 산출물을 생성할 수 있다. 또한, 설계시 고려되어야 하는 다양한 가변 요소를 사전에 안전분석 기법을 기반으로 다시 아키텍처 설계 산출물에 반영할 수 있는 방법론을 제시하였다.

차상중심 열차제어 시스템의 FMEA 안전분석 의 구조분석 자료를 바탕으로 아키텍처 구조에 대한 검증을 수행의 근거를 제공하였고, 기능분석 및 오류 분석을 통해, 기능아키텍처 산출물에 대한 검증 및 가변요소의 검증/관리 방안을 제시 할 수 있었다. 또한, 안전분석 기법의 Priority 분석 및 설계최적화 과정을 통해, Synthesis Architecture에 대한 검증을 수행할 수 있었다. 또한, 최적화된 차상중심 열차제어시스템 아키텍처의 가변요소를 고려한 설계 검증 방법을 제시하였다. 본 연구를 통해 복잡한 차상중심 열차제어시스템 시스템 아키텍처의 안전산출물을 통한 수행 가능한 검증을 통해 검증적 오류를 시스템 차원의 상위 수준에서 사전에 방지할 수 있는 효과가 있다. 이러한 FMEA 안전분석 기법 기반의 아키텍처 검증 방법론을 제시함에 따라, 설계적 신뢰도를 높일 수 있는 활동의 재정립을 통해 차상중심 열차제어 시스템 아키텍처 산출물에 대한 검증단계에 활용할 수 있는 방법을 제시하여 아키텍처 산출물의 무결성을 높여 안전성 확보를 할 수 있는 접근적 방법을 제시하였다는 점에서 기여 하였다고 판단된다.

References

[1] D.H. Shin, J.H. Baek, K.M. Lee, Y.K. Kim, "A study on the reliability management of onboard signaling equipment for the korean tilting train", Journal of the korea society for railway, vol. 12, no. 6, pp. 825-838, December, 2009.

[2] J.H. Baek, H.J. Jo, K.M. Lee, K.Y. Kim, D.H. Shin, J.H. Lee, "The study of wayside signal equipment control by ICT-based onboard", 2012th summer conference & annual meeting of the korean institute of electrical engineers, pp. 1544-1545, July, 2012.

[3] Pickard, Karsten, Peter Müller, and Bernd Bertsche (2005), "Multiple failure mode and effects analysis-an approach to risk assessment of multiple failures with FMEA." Reliability and Maintainability Symposium, 2005. DOI: http://dx.doi.org/10.1109/rams.2005.1408405

[4] ISO. "26262 – Road vehicles-Functional safety." International Standard ISO/FDIS 26262, 2011.

[5] B. Ward, "Modeling and simulation for mission-based test and evaluation (MBT&E)", in Proc. 27th Annual National Test & Evaluation Conference, Mar. 17, 2011.

[6] L. Grello, "Model based systems engineering (mbse) and modeling and simulation (m&s) adding value to test and evaluation (t&e)," in Test and Evaluation Conference, Mar. 2011.

[7] keith Phelan, Joshua Summers, and Paolo Guarneri, "Engineering change management - Verification, validation, and testing planning tool development," in Proc. Proceedings of TMCE 2014, 19-23, pp. 587-598, May 2014.

[8] Prabhu Shankar, Joshua Summers, and keith Phelan, "A verification and validation planning method to address change propagation effects in engineering design," in Proc. Proceedings of TMCE 2014, Budapest, Hungary, 19-23, pp. 635-648, May 2014.

[9] Martin, James N. "Overview of the EIA 632 standard: processes for engineering a system." Digital Avionics Systems Conference, 1998. Proceedings., 17th DASC. The AIAA/IEEE/SAE. vol. 1. IEEE, 1998.
DOI: http://dx.doi.org/10.1109/dasc.1998.741462

김 주 욱(Joo-Uk Kim) **[정회원]**

- 2000년 2월 : 고려대학교 전기공학과 (공학사)
- 2011년 2월 : 아주대학교 시스템공학과 (공학석사)
- 2016년 2월 : 아주대학교 시스템공학과 (공학박사)
- 2004년 3월 ~ 현재 : 한국철도기술연구원 광역도시교통연구본부 선임연구원 재직

<관심분야>
철도 시스템엔지니어링, 철도 안전 및 신뢰성, 아키텍처 프레임워크

오 세 찬(Sehchan Oh) **[정회원]**

- 2004년 8월 : 광주과학기술원 정보통신공학과 석사
- 2013년 3월 ~ 현재 : 아주대학교 컴퓨터 공학 박사과정
- 2004년 11월 ~ 현재 : 한국철도기술연구원 선임연구원

<관심분야>
Modular TCS, DTO/UTO 설계

김 금 비(Keum-Bee Kim) **[정회원]**

- 2011년 2월 : 서울과학기술대학교 산업대학원 전기공학과 (공학석사)
- 2014년 3월 ~ 현재 : 서울과학기술대학교 철도전문대학원 철도전기·신호공학과 박사과정 재학중
- 2014년 3월 ~ 현재 : 한국철도기술연구원 학연석박사과정 연구생

<관심분야>
철도신호통신, 정보통신

심 상 현(Sang-Hyun Sim) **[정회원]**

- 2009년 2월 : 충남대학교 나노소재공학과 (공학사)
- 2011년 2월 : 충남대학교 신소재공학과 (공학석사)
- 2013년 2월 : 아주대학교 시스템공학과 (박사수료)
- 2016년 3월 ~ 현재 : (주)에스피아이디 시스템 엔지니어링 사업부 책임엔지니어 재직

<관심분야>
시스템공학(SE), 시스템 시험평가(Systems T&E), 모델기반 시스템공학 (MBSE), Modeling & Simulation 등.

김 영 민(Young-Min Kim) **[정회원]**

- 2010년 8월 : 한국해양대학교 에너지자원공학과(공학사)
- 2016년 2월 : 아주대학교 시스템공학과(공학박사)
- 2015년 3월 ~ 현재 : (주)에스피아이디 시스템엔지니어링사업부 책임엔지니어 재직
- 2016년 9월 ~ 현재 : 아주대학교 시스템공학과 강의
- 2016년 9월 ~ 현재 : 한국철도기술연구원 광역도시교통연구본부 설계최적화 자문위원

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), Systems Safety, Systems T&E, Modeling & Simulation