Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 8 pp. 352-362, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.8.352
ISSN 1975-4701 / eISSN 2288-4688

안전분석 기법과 SysML 기반의 아키텍처 산출물의 연계성 확보를 통한 BCT 시스템의 안전 무결성 확보에 관한 연구

김주욱[1], 오세찬[1], 심상현[2], 김영민[2*]
[1]한국철도기술연구원, [2]SPID

On Ensuring the Safety Integrity of the BCT System through Linkage Safety Analysis Techniques and SysML-based Architecture Artifact

Joo-Uk Kim[1], Se-Chan Oh[1], Sang-Hyun Sim[2], Young-Min Kim[2*]
[1]Korea Railroad Research Institute, [2]SPID

요 약 오늘날 산업 기술의 발달에 따른 고도화로 인해, 최근 우리 사회에 고속열차에 이어 무인운영 도시철도에 이르기까지 다양한 열차 시스템들이 개발 및 운용되고 있는 추세에 있다. 특히, 본 연구에서 대상으로 다룬, 도시철도 도메인에서는 기존 철도차량에 대해서 신호 제어 시스템을 운용하는 환경에서 보다 복잡화된 운용개념을 지원하기 위한 신규 신호 시스템 체계의 도입이 필요로 하고 있다. 또한, 기존의 존재하지 않은 컨셉을 바탕으로 개발되는 신호 시스템은 철도를 이용하는 승객들의 인적 피해를 최소화하기 위한 노력이 필요로 하고 있다. 본 연구에서는 신규 시스템 개발에 참여하는 다양한 도메인 엔지니어로 하여금 동일한 시각 제공과 통합된 방법론을 바탕으로 효율적인 신호시스템 설계 및 안전 활동을 위한 방법론을 제시 하고자 한다. 따라서, 서로 상이한 도메인 영역의 연계성 확보를 통해 향후 신규 시스템 설계시 보다 안전성 확보를 통한 설계적 무결성을 확보할 수 있는 방법론이 될 수 있을 것이다.

Abstract Today, it appears that the rapid advances in technology have allowed broadening both the system technology and the business opportunities in the rail industry. Owing to the developments in technology and the industry, and also due to the hearth, the latest high-speed trains and a variety of unattended operations in rail systems are being developed and are operational. In particular, this study covers the existing railway rolling stock and signaling systems that operate in an environment more complex than the concept of localized management, so the introduction of a new signaling system is needed. In addition, developments based on the existing signal system concepts for passenger railways need to minimize human injury. In this study, to participate in the development of new systems in a variety of domains and to provide an integrated common vision methodology as an engineer on the basis of efficient signal system design and safety would like to present the methodology for action. Therefore, each different linkage through the next new domain zone system design: design through to secure the integrity of safety than can secure methodology.

Keywords : Signal Control System, System Safety Activity, Systems Engineering, Rail Safety, SysML

1. 서론

최근 국내 철도산업의 급격한 기술력 증대는 세계적 위상에 도약했다. 이로 인해, 국내 철도 환경은 고속열차의 대중화를 이루었다. 이는 고속열차 뿐만 아니라, 일반 노선의 열차 또한 열차 속도 증대를 가져왔다. 열차(전철

본 연구는 한국철도기술연구원 주요사업의 연구비 지원으로 수행되었습니다.
*Corresponding Author : Young-Min Kim(SPID)
Tel: +82-2-3453-5345 email: ymkim@spidconsulting.com
Received May 27, 2016 Revised (1st July 1, 2016, 2nd July 18, 2016)
Accepted August 11, 2016 Published August 31, 2016

포함)와 같이 대규모 인원들의 수송을 책임지는 교통수단(철도, 선박, 항공)과 관련해 최근에는 국내·외적으로 많은 사고가 발생하였다. 최근에도 전라선 무궁화호가 열차운전자의 과속운전을 차단하지 못하여 곡선구간에서 차량이 탈선하는 사고가 발생하였다. 이렇듯 철도 차량과 관련된 사건은 국민의 생명과 재산에 상당한 피해를 초래하기에 오늘날 안전성 확보에 대한 필요성과 중요성이 대두되고 있는 실정이다. 이와 같이, 시스템의 안전성의 문제로 인해 인명 및 재산적 상당한 피해를 입히는 대상을 안전중시 시스템이라고 불린다[1]. 따라서, 고속열차 및 전철을 포함한 철도차량은 안전중시 시스템에 속하게 된다. 이러한 철도 시스템은 크게 차량, 신호시스템, 궤도로 구성이 되며, 신호시스템의 경우, Tab. 1에서 제공하는 정보와 같이, 기존의 국내 철도차량은 지상에 위치한 통제 장치를 통해서, 특히, CBTC(Communication Based Train Control) 방식에 따른 열차 차량의 운행 및 위치에 관한 제어를 수행해 왔다.

기존의 방식으로는 지상 열차제어시스템(ATP, Automatic Train Production)에 의한 관할영역 내의 운행하는 모든 열차의 위치보고를 수신하여 이동권한과 속도 프로파일을 계산하고 이를 다시 운행 중인 열차에게 정보를 제공하는 방식 이였다. 이러한 신호제어 방식은 기존의 운용 환경에서는 안전상 크게 문제가 되지 않았다. 하지만, Fig. 1와 같이, 오늘날은 다양한 종류(고속열차, 일반열차, 경전철, 지하철 등)의 수많은 열차를 제어

Table 1. Compare Between CBTC and BCT Signal System

Composition Classification	CBTC Method Existing & Location	BCT Method Existing & Location	The main features of the components
On-board ATP	On-board	On-board	Calculate and report the location of the train, the dynamic speed profile, speed monitoring and control
Wayside ATP	Wayside	X	Calculation of the static speed profile for the move
On-board ATO	On-board	On-board	
EI	Wayside	On-board	line switcher control
ATS (Automatic Train Stop)	Wayside	Wayside	monitoring and control of train operation

하기에 기존의 방식인 지상 통제 장비에 의한 제어는 특히, 선로에서 운행 중인 열차 제어 방식은 수송의 효율성과 안전성 측면에서 문제점이 존재하고 있다. 최근 열차의 운용방식은 기술의 고도화에 따라 운행의 자동화 추세를 따르고 있다. 이에 따라 무인화 운용되는 구간도 많아지고 있다. 또한, 차량의 고속화로 인해 위험성이 가중화된 오늘날 신호시스템의 역할은 상당한 중요 역할을 차지하게 되었다. 따라서, 오늘날과 같이 보다 복잡해진 열차 운용 환경에서 수송 측면의 효율과 오류를 최소화하여 승객의 안전과 재산을 지키는 것은 오늘날 개발되는 철도 신호 시스템의 개발 및 운용 목적이 되고 있다.

고속열차의 경우, 현재의 신호 시스템의 운용 하에서 비상 상황 발생으로 인한 긴급 제동 시, 고속열차의 속도로 인해, 사고인지를 하였더라도 상당한 제동 거리가 필요하기 때문에 승객의 안전 및 재산적 피해가 유발될 수 있는 환경에 직면해 있다. 따라서, 오늘날 개발되는 신호시스템은 기존 노선에서 사용되는 신호 시스템의 효율적 운용과 승객의 안전을 보다 최우선적으로 여기기 위해서 기존 신호 시스템의 운용컨셉부터 다른 신규 시스템 개발이 요구된다. 이러한 측면에서 본 연구진은 BCT(Borderless Communication based Train control)방식의 신호시스템을 개발하고 있다. BCT 신호시스템은 기존의 신호시스템이 지상에서 차량 신호를 관제한 방식과 달리, 운행중인 차상 다시 말해, 차량 내부에 신호시스템을 갖춘 시스템을 말한다. 따라서, 국내 존재하지 않는 운용개념을 생성하고 그에 따라, 물리적 구성인 신호시스템의 설계적인 측면도 상당수 변경될 예정이다.

이러한 맥락에서, BCT 방식의 신규 신호시스템을 개

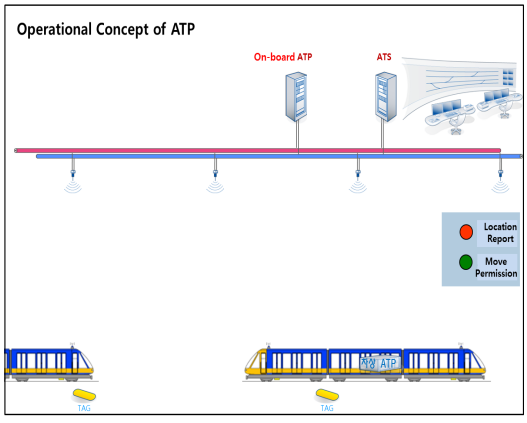

Fig. 1. Operation Concept of Existing the ATP

발하는데 있어서, 시스템 공학적 기반의 접근은 매우 유용한 학문적 접근 방법론이 될 수 있을 것이다. 시스템공학은 시스템 개발의 전 수명주기 관점에서 시스템 설계를 다루고 있지만, 특히, 개발 초기 단계인 개념설계 단계에 집중적인 활동을 통해 시스템 컨셉을 세우고 이를 기반으로 대상 시스템이 지녀야 할 기능/비기능 요구사항을 도출하여 안전성 평가까지 기여하고 있기 때문이다.

최근 개발되는 철도시스템은 고속열차 뿐만 아니라, 경전철과 같은 무인화 운용에 이르기 까지 다양한 체계로 개발 및 시스템이 구성되고 있다. 따라서, 시스템의 복잡도 증대에 따라 다양한 철도 시스템 체계를 통제하는 신호 시스템 개발 과정에서 체계적인 개발이 요구되고 있는 실정이다. 철도차량은 무엇보다 승객의 안전이 최우선시 되어야하기 때문에 개발과 관련한 모든 대상 시스템은 안전성에 상당한 노력이 필요하다. 이러한 맥락의 활동은 철도도메인 분야에서 신뢰성(RAMS, Reliability availability maintainability and safety) 활동을 통해 설계적 안전/신뢰성을 확보하기 위한 노력을 수행한다. 철도 도메인에서 안전성 평가와 관련해서는 PHL(Preliminary Hazard Analysis, PHA(Preliminary Hazard Analysis), SHA(System Hazard Analysis), SSHA(Sub-system Hazard Analysis), FMEA(Failure Mode Effects Analysis)가 시스템 수준의 안전성 평가와 관련해 중요한 관련 시스템 체계(신호 시스템 포함) 또한 개발단계에서 안전성 평가가 요구되고 있는 실정이다.

하지만, 국내 개발환경은 시스템 초기 개발단계인 개념설계 단계에서의 엔지니어링 역량이 해외 보다 낮고, 대부분의 안전성 활동 역시, 상세설계 단계에 집중되다보니, 상세설계 단계서 파생된 산출물을 기반으로 수행하다보니 설계 초기 단계에서 요구되는 안전활동(PHL, PHA, SHA, SSHA, FMEA)을 통한 안전성 평가 산출물의 품질에 대한 신뢰도가 떨어지고 있다는 게 현실이다. 이는 설계적 신뢰도에도 영향이 미칠 수 있는 사항이다.

본 연구와 관련한 선행연구로는 기존의 철도 시스템 체계에 대한 모델기반 설계적 활동은 대부분 운용 시나리오를 생성하고 이를 기반으로 시뮬레이션을 통한 검증 활동에 초점이 되고 있다. 이러다보니 실질적인 초기 설계 단계의 반영은 어려웠던 게 현실 이였다. 최근 시스템 모델링 언어 기반의 설계적 산출물은 국방/항공/자동차 도메인을 기반으로 요구되고 있는 실정이며, 철도 도메인도 마찬가지로 안전표준의 모태가 되는 ISO/IEC 61508[2]을 기반으로 안전활동이 강화되는 추세에 있다. 최근 자동차 도메인에서도 ISO 26262[3]의 등장으로 설계적 산출물과 안전성 활동의 동시적 접근을 요구하고 있다. 특히, 시스템 수준에서 표준화된 언어 기반의 설계적 산출물을 요구하고 있다. 이에 따라, 대안으로 시스템 모델링언어의 활용을 통해 국내 자동차 제조업체들이 시스템 수준에서 설계 산출물과 안전 활동을 통한 산출물을 만들어 설계적 신뢰도를 높이고 있는 실정이다.

또 다른 선행연구를 살려보면, Park(2015)는 철도시스템의 안전성 평가에 관한 기초 연구가 진행되었다. 국내 철도 시스템의 안전에 직결되는 잠재적 위험 요소를 식별하고 이러한 위험요소에 대한 평가를 수행할 수 있는 방안 및 모델을 제시하면서 국내 철도산업에서 실질

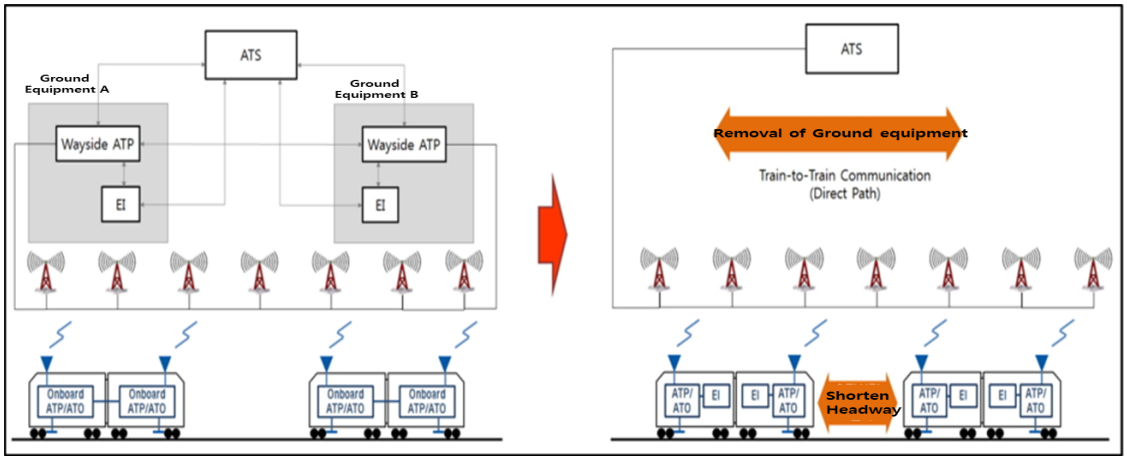

Fig. 2. The ATP System Structure of New Concept

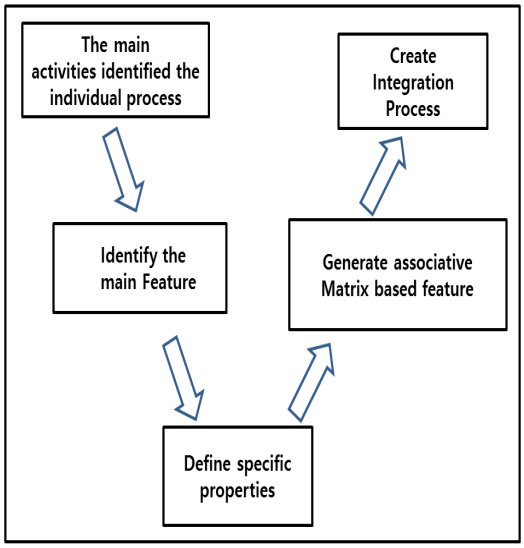

Fig. 3. A conceptual diagram representing the objectives of the paper.

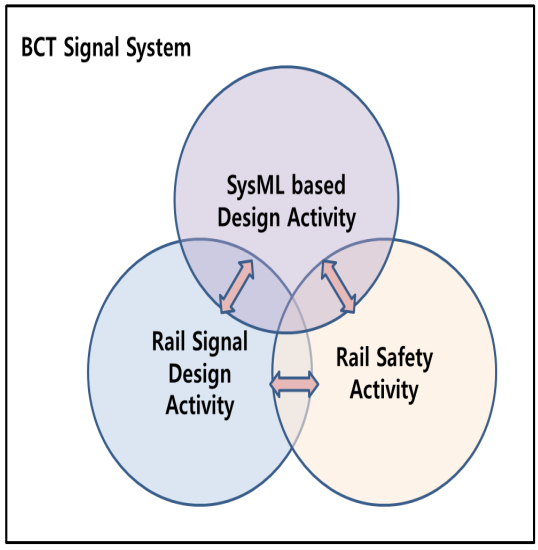

Fig. 4. The main activities for the BCT system configuration.

적인 안전성 평가 및 수행이 적절하지 못함을 선행 연구에서도 제시하고 있다. 특히, 대부분의 연구에서는 안전성 측면에서만 접근하려고 하며, 본 연구에서 제시하려고 하는 설계적 관점에서의 연동적 측면에서는 제시하지 못한다는 점에서 한계점으로 인지할 수 있는 부분이다.

본 연구와 상당히 밀접한 연구를 수행한 시스템 설계와 안전성 평가를 동시 수행을 위한 연구가 수행되었다. Kim(2012)는 일반 설계적 관점에서 시스템 설계의 개념설계 단계에서 요구하는 설계활동과 산출물을 명시하였고, 같은 수명 주기 내에서 요구되는 안전성 활동과의 매칭을 통해 동시공학 측면에서의 수행방안을 제시하였다. 하지만, 본 연구에서 다루는 철도 신호 시스템이라는 특수 분야에 국한하여 적용하기에는 적합하지 않다. 따라서, 본 연구를 통해 보다 해당 도메인에서 요구하는 특성을 반영하여 적용 가능하도록 제시하였다. 또한, 철도 신호 시스템 개발에서 요구하는 안전활동 그리고 국제 표준접 접근을 위해서 시스템 모델링 언어라는 기준이 되는 접근을 기반으로 동시 공학적 접근이 될 수 있는 방안을 제시 하였다.

국내에서 BCT라는 신규 개념이 반영된 신호 시스템을 개발하는데 있어서 오늘날 철도 차량 신호제어 시스템도 마찬가지로 복잡화된 대형화 추세의 개발 환경 속에서 과거의 단일 시스템과 달리 매우 복잡한 대형 시스템에 적용하기에 한계에 이르렀다[6],[7]. 따라서, 본 연구에서는 운용개념이 복잡한 신호시스템의 개발이라는 목표달성을 위한 접근으로 기존의 지상에서 운용되었던 기능과 물리적 구성품이 차량으로 설계적 구현이 되기 위한 접근적 방안이 필요한 시점에 와있다.

본 연구에서는 BCT 신호 시스템의 개념설계 단계에서 요구되는 설계활동. 설계 산출물, 그리고, 안전 활동, 안전 활동에 따른 산출물을 상호 유기적 활용을 제안하고자 한다. 이를 통해, 신규 개념을 지니고 개발하는 BCT 신호 시스템 개발에 대한 설계 및 안전성 평가의 엔지니어링 역량을 Fig. 4에서 제시하는 바를 근간으로 효율적이고 체계적인 접근할 수 있는 방안을 제시하고자 한다. 설계적 측면에서는 국제 표준 모델링 언어인 시스템모델링 언어의 활용과 안전측면의 안전성 평가 또한 시스템 수준에서 요구되는 안전 활동을 기반으로 상호 두 활동의 유기적 관계를 제시하고자 한다. 이러한, 설계와 안전이라는 상이한 도메인 분야에 대해서 시스템 수준에서 동일한 시각과 수행적 측면에서 보다 효율적으로 접근할 수 있는 방안을 제시 하였다.

본 논문에서의 주요 활동은 Fig. 3과 같으며, 본 연구에서 철도 차량의 신호 시스템을 대상으로 신규 개발 시 요구되는 설계 활동과 안전활동을 동시적 접근을 통해 수행할 수 있는 방안을 제시 하였다. 따라서, 동일한 수명주기를 대상으로 상호 연동성을 제시 하였고, 특히, 국제표준 모델링 언어인 시스템 모델링 언어의 활용을 통

해 상이한 도메인 전문가의 활용성을 높이도록 하였다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 언급하였다. 3장에서는 기존 신호시스템 설계 활동과 안전활동에 따른 수행 방법을 속성 기반으로 분석하였고 이를 상호 연동성 분석을 통해 연동성 분석을 수행하고자 한다. 4장에서는 제시된 접근법을 시스템모델링언어와의 연동성 분석을 통해 수행 가능한 방안을 제시 하여 모델기반 설계 및 안전활동 가능한 절차 및 방안을 확립 및 적용하였다. 5장에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 문제의 정의

2.1 안전분석 기법과 아키텍처 설계 산출물의 연계성 확보의 필요성

시스템의 설계단계를 Kossiakoff(2011)는 Concept Development, Engineering Design, Post Engineering이라는 3단계로 규정하고 있다. 운용시나리오는 초기 설계 단계인 개념설계 단계에서 이해당사자로부터 수집한 정보와 요구사항으로부터 시스템 거동의 상위수준에서 생성된다. 오늘날과 같이 고도화된 복잡한 수많은 하부체계로 구성된 대형 시스템을 개발하는데 있어서 최근 개념 설계 단계에서 활동이 부각되고 있다. 대형 시스템의 개발환경에서 초기 설계 수행 활동의 중요성이 부각되면서 체계적 설계에 관한 많은 연구들이 진행되고 있다[9].

시스템 수준에서 수행해야하는 설계활동의 산출물과 안전활동에 필요로 하는 입·출력 산출물에 상당수 시스템 수준에서 식별된 설계 자료들이 근간으로 필요로 한다. 따라서, 초기 설계 단계에서부터 설계적 측면과 안전성 측면의 상호 연동성에 관한 수행의 필요성이 오늘날 대형 복합 시스템을 기반으로 확산되고 있는 추세이다. 본 연구에서는 이러한 상이한 도메인 영역을 하나로 통일화된 접근 및 시각을 갖기 위해서 개별영역에서의 활동과 산출물이 지닌 휘쳐(특성)과 속성을 기반으로 연계성을 확보하였다.

2.2 시스템모델링언어 기반의 설계 및 안전분석 기법의 통합 수행의 필요성

오늘날 개발되는 시스템은 다양한 고객의 요구를 충족시키기 위해서 수많은 기능이 탑재된다. 특히, 이러한 다양한 기능적 부분의 구현에 대해서 소프트웨어가 많이 관여하는 추세에 와 있다. 이렇다 보니, 개발되는 대다수의 시스템이 소프트웨어 중심 시스템의 형태로 개발되는

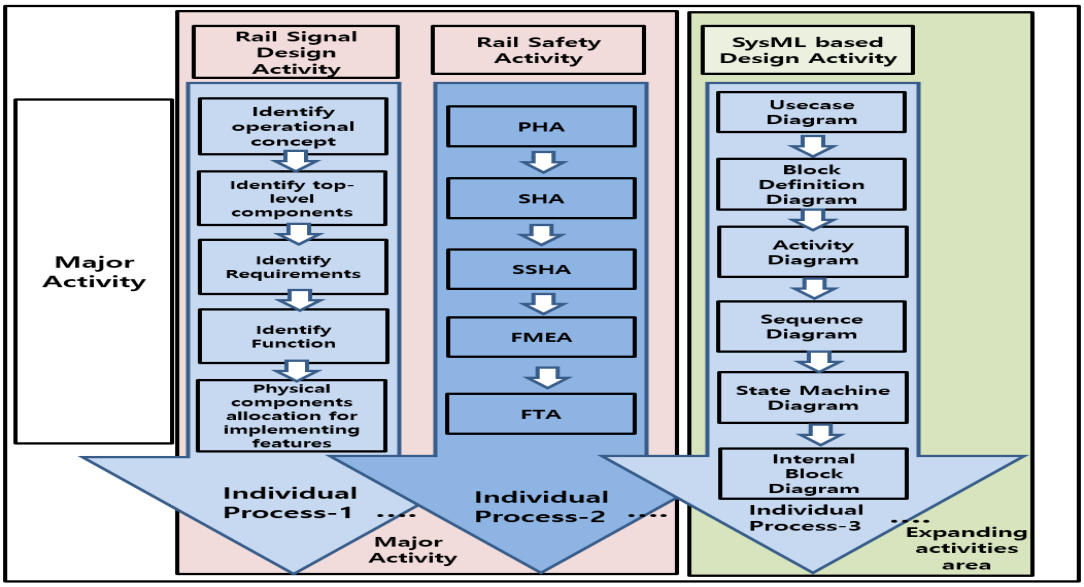

Fig. 5. The main activities of the individual processes.

추세에 있다. 과거에 단순 하드웨어 중심의 시스템 체계로 이루어 졌다면, 오늘날 개발되는 시스템의 형태는 다학제적 접근이 결집된 소프트웨어 중심의 시스템 체계로 구성되고 있다. 따라서, 오늘날 올바른 시스템을 개발하기 위해서는 시스템, 하드웨어, 소프트웨어 영역에 이르는 모든 영역, 즉 다학제적인 접근의 조화로운 활동을 기반한 시스템 설계 및 안전 활동이 필요로 한다. Fig. 5를 통해서 알 수 있듯이, 서로 독립적인 영역으로 여겼던 영역에 대해서 시스템모델링언어 기반의 접근을 통한 공통의 접근 방안을 찾는다면 오늘날 복잡화된 대형화 시스템 개발에 적합한 방법론으로 활용할 수 있을 것이다.

2.3 연구 목표 및 범위

상위 선행연구 분석을 통해, 기존에 신호 시스템 설계 및 안전 활동을 수행하는데 있어서 상호 독립적인 수행되어 왔다. 기존의 신호 시스템을 개선하는 사항도 아닌 신규 컨셉의 신호 시스템을 개발하는데 있어서 설계적 측면과 안전성 측면에서 위험성이 존재하고 있다. 따라서, 보다 설계적 무결성을 높임으로써 신호 시스템의 안전성을 확보할 수 있는 상황이다. 본 연구에서는 제약적인 개발환경에서 신호 시스템 개발의 보다 효율성을 높이고 설계적 데이터를 기반한 안전 분석 방안을 시스템 모델링 언어라는 공통의 언어를 바탕으로 구현 및 이행할 수 있는 방법론을 제안 하고자 한다. 본 연구는 개념설계단계에서 요구하는 신호 시스템 개발과 안전분석 활동을 중심으로 대상의 범위를 한정하고자 한다.

3. 설계/안전활동 및 산출물의 속성 기반 상호 연동성 구축

3.1 개별 도메인 개발 프로세스 및 주요활동 식별

기존 개별 도메인 영역인 신호시스템 설계, 신호 시스템 안전 활동은 서로 상이한 영역을 하나의 동일한 시각으로 제공하기 위해서 우선, 개별 도메인에서 요구하는 설계적 프로세스 및 활동을 식별하였다.

이렇게 식별된 개별 도메인 활동은 활동의 속성값을 활용한 상호 연동성 확인에 중요한 지표가 된다. Fig. 5에서 제시되는 바와 같이 개별 도메인 활동에서 요구하

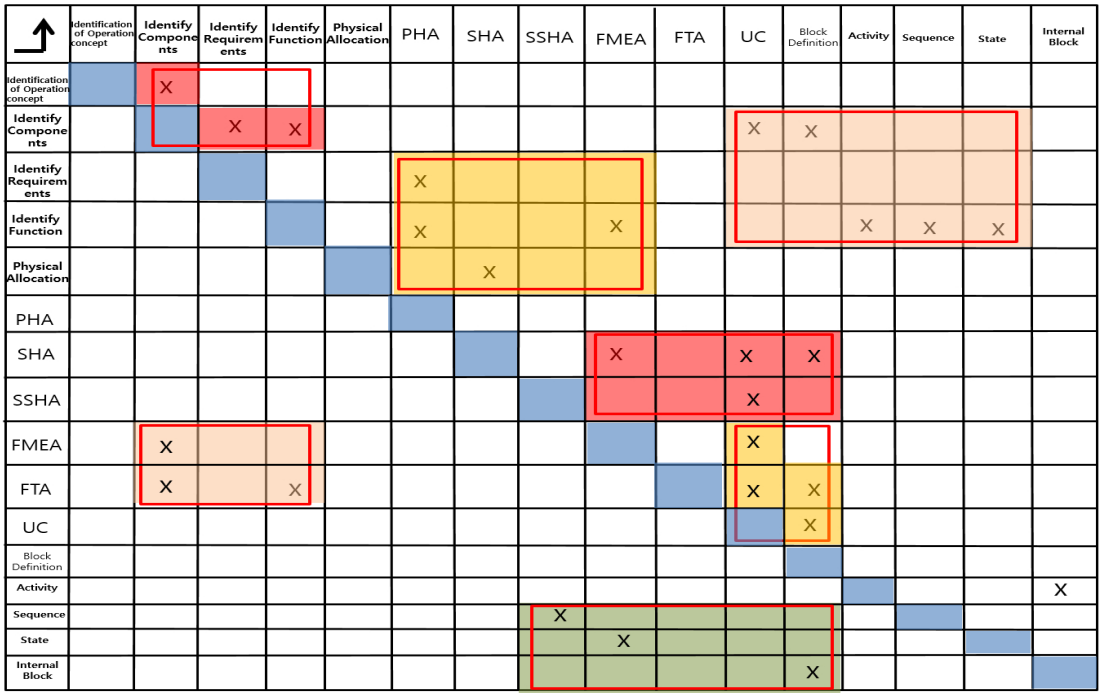

Fig. 6. The Matrix for Process linkage analysis.

는 활동을 명시하였다. 지금의 활동은 개별 도메인에서 독립적 수행을 해왔기 때문에 상호 어떠한 요소(활동 또는 산출물)과 연동성이 있는지 확인이 어려웠다. 이러한 문제점을 개선하기 위해서 다음과 활동을 기초로 수행하였다.

Step 1. 신호시스템의 개념 설계단계에서 요구되는 주요 설계 활동을 식별하였다.

Step 2. 신호시스템의 안전성 활동, 특히, 시스템 레벨에서 요구하는 안전 활동을 분석하여 식별하였다.

Step 3. 시스템모델링언어의 활용시 사용되는 활동을 이행하기 위한 다이어그램을 식별 하였다.

3.2 식별된 요소의 상호연동성 반영을 위한 속성 분석 및 연동성 확인

본 연구를 통해 신호시스템 개발 시 요구되는 설r계적 활동과 안전활동/산출물의 연동성을 분석하기 위해서 앞선 3.1절의 활동을 통해서 식별하였다. 본 절에서는 식별된 해당 활동 및 산출물이 지니고 있는 휘처(특성) 및 고유의 속성 정보 값을 식별하였다. 식별된 정보를 바탕으로 유사한 성향을 지닌 요소간의 연동성 확인을 수행하였다. 따라서, Table. 2과 같이, 개별 도메인 활동에서 요구하는 활동 및 프로세스를 기반으로 휘처와 속성 값을 식별하여 정의 하였다.

또한, 식별된 정보를 바탕으로 Fig. 6에서 제공하는 바와 같이, 개별 활동 및 산출물이 지니고 있는 휘처와 속성 정보 값을 바탕으로 상호 연동성을 확인하기 위한 Matrix 기법을 활용해 분석하였다.

이러한 연동성 확인의 결과를 바탕으로 기존에 개별 프로세스가 상이한 활동으로 여겨져 개별적 수행을 해왔다면, 본 연구 단계를 통해, 상호 어떠한 요소 또는 활동과 연동성이 있는지 파악 할 수 있는 접근이 되었다. 따라서, 설계적 접근과 안전성 측면의 수행 활동을 하나의 접근 방안을 토대로 수행할 수 있도록 Fig. 7과 같은 통합 연동 프로세스를 구축하였다. 이를 기반으로 신호시스템 설계 / 시스템모델링언어 / 철도 안전 활동을 일관된 활동이 될 수 있도록 연동 기반의 수행 방안을 제시하였다.

Table 2. The main properties of the individual process-specific

Major Activity & Artifact		Feature	Attribute
Design of On-board ATP	Identify Operation Concept	Operational Scenario	Concept
	Identify Component	Structure, Components	Structure, Component
	Identify Requirements	Requirement	Function, None-function
	Identify Function	Function	Function, Action
	Physical Allocation	Physical Allocation	Component, Allocate
Rail Safety Activity	PHA	Pre-hazard Analysis	Hazard
	SHA	System Safety Analysis	System, Hazard
	SSHA	Sub-systems, Safety Analysis	Sub-System, Hazard
	FMEA	Failure Mode, Structure and Function Analysis, Effect Analysis	Failure Mode
	FTA	Fault Analysis, Hazard Cause	Fault Effect Probability
Model-based Design	UseCase	Operational Scenario	Concept, Function
	Block Definition	Physical Components	Block
	Activity	Action, Sequence, Inter-operability	Action, Interface
	Sequence	Single or Multi-object, Inter-Operability	Sequence, Interface
	State	Single Component, State	State
	Internal Block	Internal Component	Block, Component

4. 시스템 모델링언어 관점에서의 시스템 설계 및 안전활동 통합수행 사례

4.1 구축된 설계/안전 통합 프로세스의 프로세스에 의한 신호시스템 설계 수행

Fig. 5에서 제시하는 서로 다른 영역의 활동을 속성 기반의 정보 값을 바탕으로 Fig. 7과 같이, 하나의 통합된 방법론이 제시되었다. 제시된 통합 연동 프로세스 모델을 시스템모델링언어를 기반으로 Fig. 8과 같이 모델 기반 설계 및 안전 활동을 수행하였다. 유스케이스 다이어그램을 통해, BCT 신호 시스템과 연계된 이해당사자를 식별하고 관련한 기능을 정의 할 수 있었다. 이러한 정보를 바탕으로 시스템의 계층에 따른 신규 신호 시스템의 체계 구성도에 대한 초안을 생성 할 수 있었다. 생성된 초기 시스템 구조 자료는 FMEA 등 다양한 안전활동 수행에 입력 자료로 활용되었다. BCT 시스템을 구성하는 개별 하부 시스템들의 개별 거동을 분석을 통해 보다 구체화된 기능을 식별하고 이를 기반으로 인터페이스 정보를 식별하기 위해서 Sequence, Activity, State Machine 등 동적 거동 분석지원이 가능한 다이어그램의 활용을 통해 보다 상세화 된 분석을 수행하였다. 분석된 기능, 기능 수행에 따른 데이터 연동 정보를 바탕으로 안전 활동에 직결되는 활동 그리고 상호연동성에 대한 분석을 통해, 개별 기능 기능의 오작동으로 발생할 수 있는 영향 분석이 가능하게 되었다. 초기 시스템 구성을 식별하기 위한 유스케이스 다이어그램의 사용에 따른 물리적 구성품 한계점을 거동분석 자료를 기반으로 보다 점진된 보완을 수행하였다. 최종적으로 Fig. 8 우측 최상단에 위치한 Internal Block Diagram의 활용을 통해 보다 정형화된 BCT 신호시스템이라는 신규 신호 시스템의 물리적 구성을 도출할 수 있었다.

4.2 시스템모델링언어 기반 산출물의 안전활동 속성값 정보를 활용한 산출물 연계활동

시스템모델링언어가 가진 개별 속성정보 값과 철도안전 활동에서 요구하는 산출물의 개별 항목이 지니고 있는 속성정보의 일치화 과정을 통해 Fig. 9와 같이, 안전 활동 산출물 생성에 필요한 입력 값을 식별하여 안전활동 산출물을 생성하였다. 산출물 연계활동을 수행하기 위해서 기존 안전 활동 산출물의 템플릿을 기반으로 개별 템플릿이 지니고 있는 항목을 분석하고 개별 항목이 지닌 고유의 속성 정보를 분석 하였다. 분석된 속성 정보 값을 살펴보면, 시스템의 구성(Element), 해당 구성품의 오류 발생 원인(cause), 오류의 형태(Mode), 오류 발생으로 미치는 영향(effect)에 관한 정보 값을 필요로 했다.

BCT 신호시스템의 시스템모델링언어를 통한 구현한 산출물을 바탕으로 모델링언어를 통해 구성된 개별 객체가 가진 속성정보를 활용하였다. 시스템모델링언어를 통해 BCT 신호 시스템의 구조적 정보를 표현한 산출물은 안전활동의 시스템 구성품에 연계되었다. 또한, 거동적 표현을 지원하는 다이어그램의 활용을 통해서 표현된 개별 객체는 지니고 있는 기능(거동)정보와 인터페이스 정

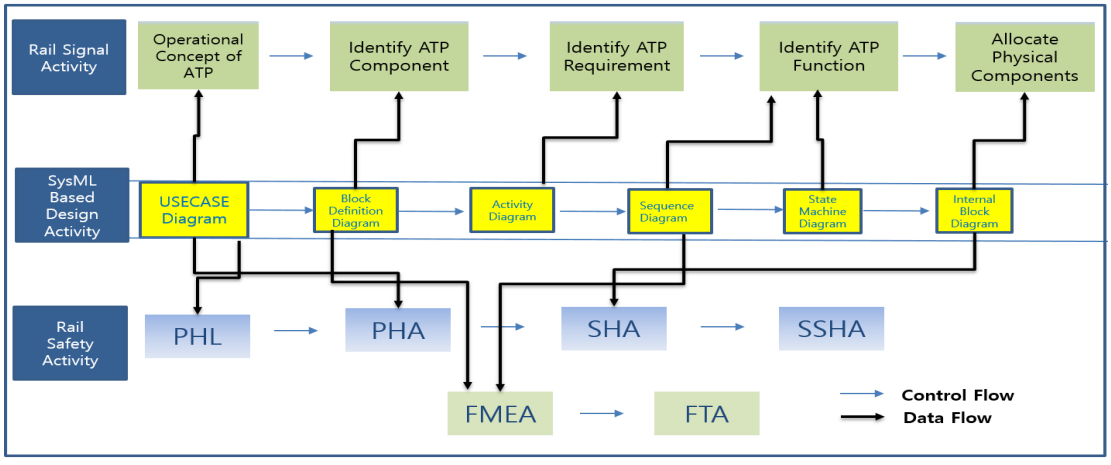

Fig. 7. Build a property-based inter-operability Process.

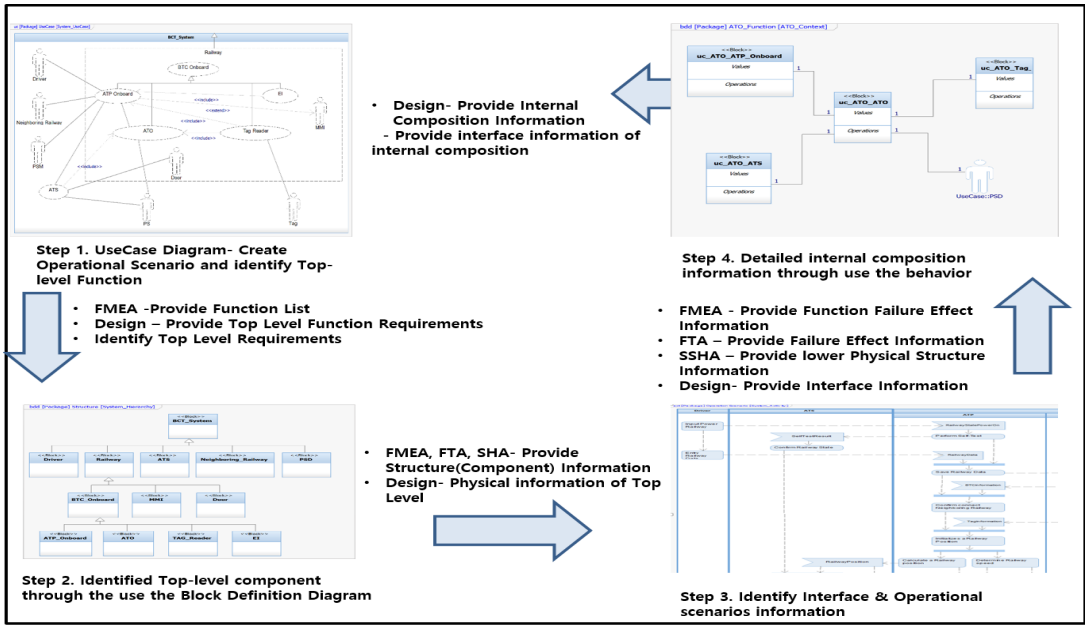

Fig. 8. The proposed process-based applications case.

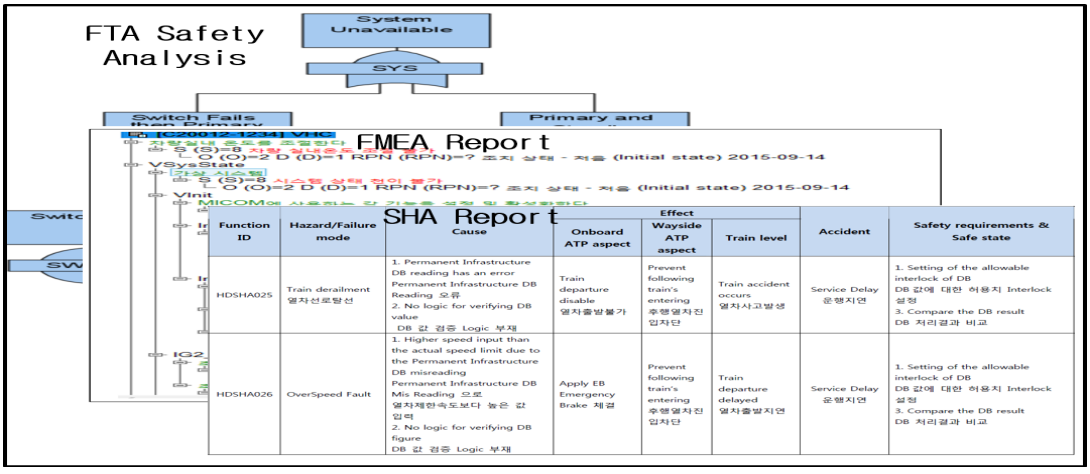

Fig. 9. The Major artifact of safety activities.

보를 바탕으로 안전활동 수행에 필요한 원인, 모드, 연계된 오류(영향)에 필요한 정보를 제공할 수 있게 되었다.

5. 연구결과

국내 철도분야에서는 설계와 안전성 확보를 위한 노력이 연장선에서 일원화되어 수행되지 못하는 상황에 있다. 따라서, 철도 안전분석 활동 수행 시, 입력자료로 어떠한 데이터를 활용할지에 대한 많은 어려움을 겪고 있다. 본 연구를 통해, 모델기반 설계적 활동에 따른 산출물을 기반으로 신규 신호시스템의 안전성 확보를 위한 노력이 본 연구를 통해 수행되었다. 특히, 설계활동/산출물, 안전활동/산출물이 지니고 있는 속성적 정보를 가지고 시스템모델링언어를 구성하는 개별 객체와의 속성적 연계성 확보가 가능하게 하였다.

따라서, 시스템 모델링언어를 활용해, 구조적/기능적 분석이 수행되었다. BCT 신호시스템의 구성에 관한 큰 틀에서 Block Definition 다이어그램을 활용하여, ATS, ATP, EI, Tag, 등 상위 수준의 구성품이 식별되었고, 보다 상세적인 구조는 Internal Block Definition 다이어그램의 활용을 통해 보다 상세화된 내부구조를 식별하였다.

시스템모델링언어의 활용을 통해 초기 구조적 분석을 수행하였고, 이러한 구조적 관점의 산출물은 Fig. 9와 같이, 안전분석 FMEA, SHA, PHA 수행시트의 구성품에 해당되어 그대로 구성품에 대한 입력 자료로 활용하였다. BCT 신호 시스템의 구조적 분석결과를 바탕으로 식별된 구성품은 Usecase/Sequence 등 거동분석을 지원하는 다이어그램의 활용을 통해 안전분석에서 요구하는 기능의 오류시 발생될 수 있는 영향에 대해서 분석 가능한 정보를 제공하였다. 열차제어시스템 ATP의 기능적 식별 활동을 통해, 무선통신을 기반으로 선로변 정보제공 기능, 열차이동권한 부여 기능, 열차의 위치 및 속도검지를 위해 필요시 되는 기능적 측면의 거동 분석을 수행하였다. 따라서, 개별 거동이 수행되는 다양한 모드(Mode)적 관점에서 발생될 수 있는 기능적 오류를 식별하여 이로 인한 영향을 안전분석 수행 시트에 입력 자료로 활용하였다.

따라서, 본 연구수행을 통해, 모델기반 설계 산출물을 바탕으로 안전분석 수행이 가능한 접근이 가능한 방법론을 제시하였다. 본 연구는 시스템 상위 수준에서 모델기반 방법론으로 시스템 설계와 안전 활동을 병행적 수행 가능한 방법론을 제공함에 따라 향후, 설계와 안전의 통합적 접근에 관한 연구활동의 기초를 제공하였다. 후속, 연구는 객체 속성 정보를 보다 상세화하여 연구 범위를 확대 하고자 한다.

References

[1] 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.

[2] ISO, EN. "IEC 61508." Functional Safety of Electrical/Electronic/Programmable Electronic Systems Part 1 (1998): 1998-2001.

[3] Hillenbrand, Martin, et al. "ISO/DIS 26262 in the context of electric and electronic architecture modeling." Architecting Critical Systems. Springer Berlin Heidelberg, 179-192. 2010.
DOI: http://dx.doi.org/10.1007/978-3-642-13556-9_11

[4] M. G. Park, W. Y. Gee, and S. W. Shon, “A study on the risk assessment of the railway system”, Korean Reliability Institute, pp. 53-59, 2015.

[5] Y. M. Kim and J. C. Lee, “On the Integration of Systems Design and Systems Safety Process from an Integrated Data Model Viewpoint,” Korea Safety Management & Science, vol. 14, pp. 107-116, 2012.
DOI: http://dx.doi.org/10.12812/ksms.2012.14.4.107

[6] B. G. Joo, G. J. Park, S. W. Lim, and C. G. Cha, “Preliminary Hazard Analysis for Near Surface Transit Signal System”, Institute of korean electrical and electronics engineers, vol. 64, pp.97-103, 2015.

[7] E. G. Lee, et al. "Development of the Traffic Signal Control Strategy and Signal Controller for Tram" Journal of Korean Society of Transportation 33.1, pp. 70-80, 2015.
DOI: http://dx.doi.org/10.7470/jkst.2015.33.1.70

[8] A. Kossiakoff, W. N Sweet, S. Seymour, and S. M Biemer, Systems engineering principles and practice. vol. 83: John Wiley & Sons, 2011.
DOI: http://dx.doi.org/10.1002/9781118001028

[9] Y. M. Kim and J. C. Lee, “On the Use of Models in the Conceptual Design of Unmanned Aerial Vehicles,” Korea Institute of Communication and Information Sciences" vol. 37, pp. 206-216, 2012.
DOI: http://dx.doi.org/10.7840/KICS.2012.37C.2.206

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

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

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 에너지지원공학과(공학사)
- 2016년 2월 : 아주대학교 시스템공학과(공학박사)
- 2015년 3월 ~ 현재 : (주)에스피아이디 시스템엔지니어링사업부 책임엔지니어 재직

<관심분야>
철도/국방 시스템엔지니어링, Model-Based SE (MBSE), Systems Safety, Systems