J. Korea Saf. Manag. Sci. Vol. 16 No. 1 March 2014
http://dx.doi.org/10.12812/ksms.2014.16.1.79

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

SysML을 활용한 기능안전 기반의 위험원 분석 방법

정 호 전* · 이 재 천*
*아주대학교 시스템공학과

On a Hazard Identification Method Based on Functional Safety and SysML

Ho Jeon Jung* · Jae-Chon Lee*
*Dept. of Systems Engineering, Ajou University

Abstract

The rapid growth of complexity and scale can be witnessed in the design and development of modern systems. As such, the severity of damages in the occasional accidents has attracted great deal of attention lately. Although a variety of methods have so far been studied to overcome or reduce the disastrous results of hazards, the issues seem still persistent and even complicated due to the situation mentioned above. The concept of functional safety has been regarded as one approach to handling the matters by shifting up to the functions level from the consideration of each physical component itself. The outcomes of those efforts would be the international standards on functional safety such as IEC 61508 and its relatives including IEC 62278, EN 50128, ISO26262, and so on. In this paper, a method of how hazards can be analyzed to be coped with those standards has been studied. In the method proposed, the systems modeling language (SysML) is playing a key role to model and analyze the hazards from the viewpoint of functional safety. The approach taken has been applied in the analysis of the hazards in railroad systems. In spite of focusing on the individual components hazards, the method based on functional safety has analyzed them collectively with the added effect of identifying the cause originated from the interface between the functions.

Keywords : Safety, Hazard Analysis, Systems Engineering, SysML, Functional Safety, IEC 61508

1. 서 론

오늘날 기술의 발전으로 시스템들은 점차 대형화 복잡화 되어가고 있다. 이처럼 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 특히 이런 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다. 국방, 철도, 항공, 해양, 원자력 등의 안전이 중시되는 산업분야에서는 안전과 관련한 표준규격을 제정하고 이를 준수하도록 권장하고 있다. 또한 현대의 시스템에서 전기전자 및 소프트웨어의 비중이 높아지면서 전기전자 기능안전성 규격(IEC 61508)이 제정되어 현대시스템의 안전에 관한 규격을 제시하고 있다.

† 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2012R1A1A2009193)
† Corresponding Author : Jae-Chon Lee, Dept. of Systems Engineering, Ajou University
San 5-1, Woncheon-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do, Korea
M · P : 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received January 20, 2014; Revision Received March 11, 2014; Accepted March 19, 2014.

이를 바탕으로 하여 안전이 매우 중요시 되는 각 산업분야의 특성에 맞게 개선하여 자동차, 원자력, 의료기기 등의 산업분야에서 기능안전성에 관한 표준이 제정되어 이에 따른 시스템의 개발을 권고 하고 있다. 이와 같이 안전은 여러 산업분야에서 시스템의 개발에 있어서 반드시 확보해야 할 필수 요소가 되었으며, 이를 위한 투자가 활발히 이뤄지고 있다.

이처럼 중요시되고 있는 안전의 확보를 위해 제시되고 있는 많은 표준규격에서 안전을 위한 첫걸음으로 제시하고 있는 것이 위험원 분석(Hazard Analysis)과정이다. 위험원 분석은 시스템에 내재되어 있는 위험원들을 식별하고, 향후 위험원에 의해 발현될 위험들을 미리 예상하고 평가하여, 이에 대한 대응을 수립하는 것을 포함하는 과정이다. 안전관련 표준에서는 위험원 분석을 시스템 개발의 초기에 수행함으로써 목표로 하는 안전수준에 도달 할 수 있다고 제시하고 있다.

참고문헌[1]~[2]에서 제시하고 있는 현재의 위험원 분석 과정을 살펴보면, 위험원 분석이 부품 및 장치 수준을 중심으로 이뤄지고 있음을 알 수 있다. 이는 물리적인 부품 및 장치로 인한 위험원의 식별 및 위험평가가 현재 위험원 분석의 주요 목표라는 것을 반영하고 있는 것이다.

하지만 현대의 시스템에는 전기, 전자 장치 및 소프트웨어의 비중이 높아지고 있다. 특히 안전과 밀접한 관련이 있는 제어시스템에서 더욱 전기, 전자 장치의 비중이 커지고 있다. 그러나 현재의 부품 및 장치 중심의 위험원 분석은 전기, 전자 장치 및 소프트웨어에 대한 적절한 접근 방법이 아니다. 따라서 IEC 61508, ISO26262등의 기능안전 표준을 충족하기 위한 적절한 위험원 분석 방법이 필요하다. 이를 위해 시스템의 개발초기에 요구사항 분석, 기능분석 등을 포함하는 시스템에 대한 체계적인 분석을 바탕으로 한 위험원 분석이 수행되어야 한다.

참고문헌[3]에서는 위험 분석을 위해 시스템공학적 접근 방법을 제시하고 있다. 시스템 공학 프로세스인 요구사항 분석, 기능분석을 통한 위험원의 식별 방법을 제시하고 있다. 시스템에 대한 요구사항을 도출하고, 각 요구사항을 구현하기 위한 모든 기능을 식별한다. 식별된 모든 기능들에 대해서 각 기능들이 오류를 일으킬 경우를 위험으로 정의하고 있다. 그러나 요구사항의 분류, 각 요구사항을 통해 도출할 수 있는 기능의 형태에 대해서만 제시하고 있으며, 이를 바탕으로 단순히 식별된 기능들을 나열한 수준에 그치고 있다.

단순히 기능을 식별하여 나열하는 것이 아니라 기능을 구조적으로 분석하여 위험원을 식별함으로써 하나의 기능이 다른 기능에도 영향을 미칠 수 있다는 것을 파악 할 수 있을 것이다. 또한 상위수준인 시스템 수준에서부터 체계적으로 기능을 식별함으로써 단순히 부품, 장치수준에서의 위험이 아닌 시스템 수준에서의 위험의 대응이 가능 하다. 또한 현대의 시스템의 복잡성이 증가함에 따라 개별 기능에 대한 위험원뿐만 아니라 여러 기능이 서로 연관되어 인터페이스 상에서 발생할 수 있는 위험원들의 식별이 필요하다.

본 논문에서는 상위수준에서부터 Top-down 접근을 통한 기능분석을 수행하고 이를 바탕으로 위험원의 식별을 수행하며 또한 SysML을 활용하여 기능들 간의 인터페이스를 분석하여 인터페이스 상에서 발생할 수 있는 위험원에 대해서도 분석이 가능하도록 하였다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 위험원 분석단계에서의 SysML의 활용에 대한 방법론을 제시한다. 4장에서는 3장의 활동을 바탕으로 도출된 위험원 분석 방법에 따른 철도 시스템에 대한 위험원 분석 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약 하였다.

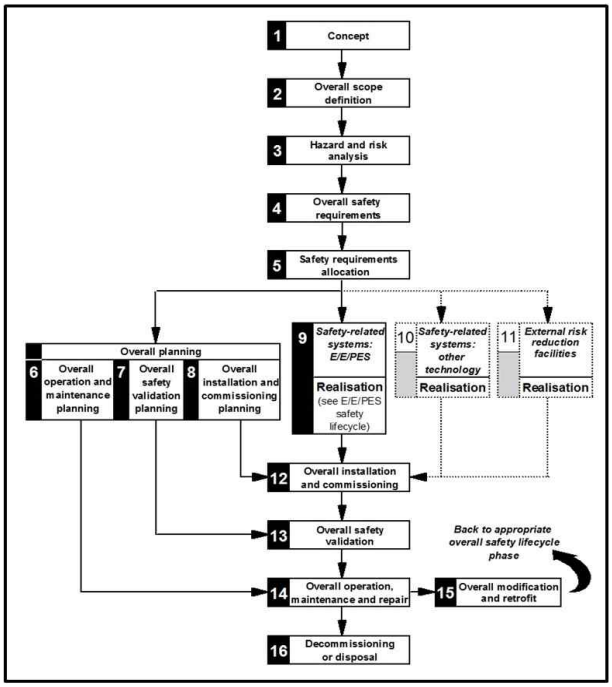
2. 문제 정의

2.1 시스템 개발에서 위험원 분석의 중요성

위험원 분석단계는 기능안전표준에서 제시하고 있는 안전관리 절차에서 위험관리 단계에서 수행되는 활동이다. 기능안전표준에서 제시하고 있는 안전관리절차의 목표는 위험을 식별하고 허용 가능한 범위 내에서 통제하는 것을 의미한다. 이에 따라 <Figure 1>과 같이 기능안전표준에서는 안전 수명주기에서 위험원 분석절차를 포함하고 있으며, 위험원 분석단계에서 사고 및 고장의 근본 원인인 위험원을 식별하고, 향후 발생 할 수 있는 위험에 대한 대응책을 수립하도록 제시하고 있다.

기능안전 표준에서 제시되고 있는 위험원 분석 절차를 분석해보면 <Figure 2>와 같이 대상 시스템을 분석하는 것에서 시작하여, 위험원을 식별하고, 식별된 위험원을 평가하고, 위험원에 의해 발현될 위험을 평가하고 통제하는 단계 등을 포함하고 있다. 즉 기능안전 표준에서 정의하는 위험원 분석은 개발되는 시스템에 내재하고 있는 잠재적 위험원을 찾아 제거하거나 위험

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)



<Figure 1> Safety life-cycle in functional safety standard[4]

원으로 인해 발생하는 위험을 허용수준 이하로 줄일 수 있도록 대책을 수립하는 것이다. 또한 이를 시스템의 설계 및 개발에 반영하도록 하는 모든 일련의 활동을 의미한다.

이와 같이 기능안전표준들에서는 시스템의 개발에 따라 안전 활동을 수행하여 안전의 확보를 달성 할 수 있도록 제안하고 있다. 더불어 이러한 안전 활동의 핵심이자 첫 단계로써 위험원 분석단계를 제시하고 있다. 따라서 시스템의 안전의 확보를 위해서는 대상 시스템에 대한 체계적인 위험원 분석이 매우 중요하다.

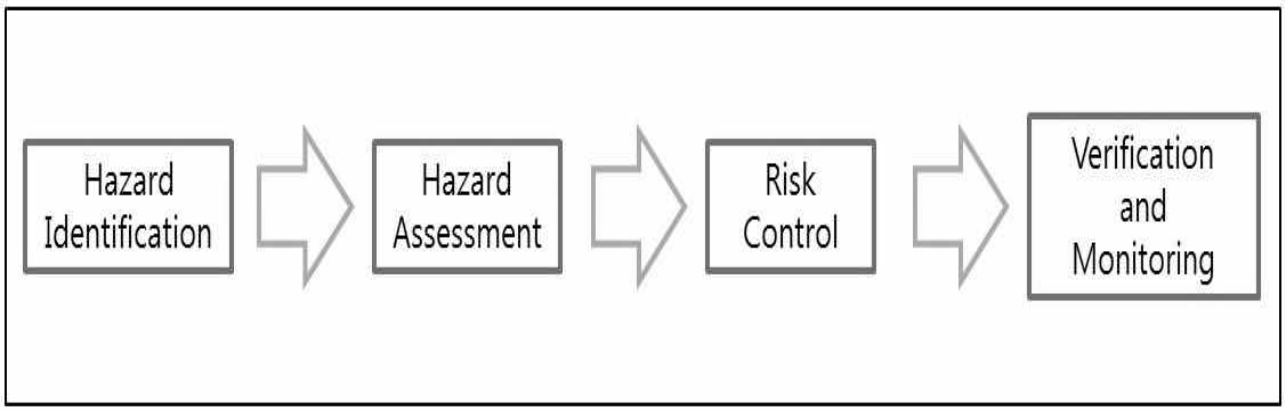
2.2 위험원 분석단계에서의 SysML의 활용성

2.1 절에서 제시한 것처럼 시스템의 개발에 있어서 안전의 확보를 위해서는 위험원 분석의 수행이 매우 중요하다. 그러나 현재의 위험원 식별 기법들은 시스템의 하부수준인 부품 및 장치수준에서의 위험원 식별에 치중되고 있다.

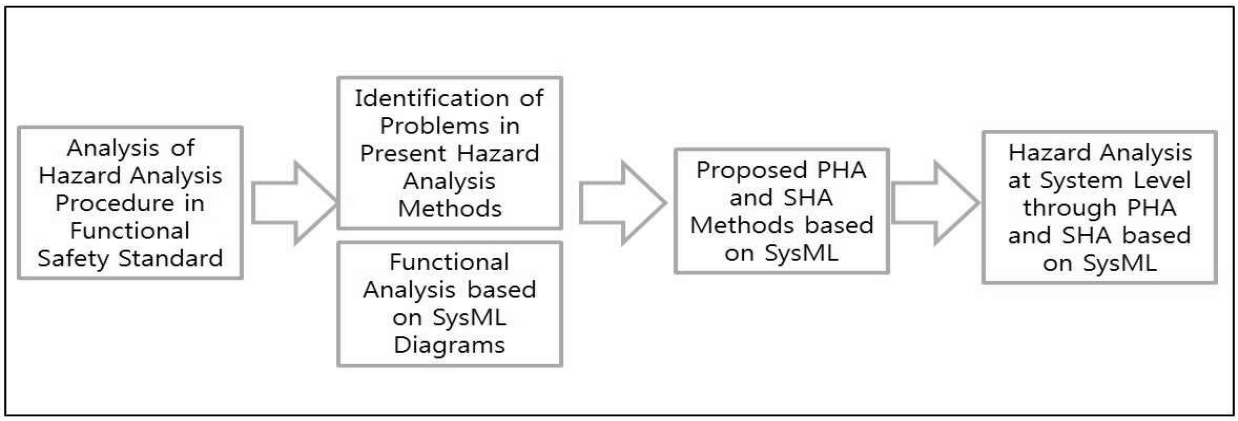
하지만 ISO26262와 같은 기능안전표준에서는 시스템 수준에서의 위험원의 식별을 수행하도록 명시하고 있다[5][6]. 복잡성이 증가하고 있는 현대의 시스템에 대해서 현재와 같은 부품 및 장치수준에서의 위험원 분석은 위험원 누락의 위험이 존재하게 된다[7][8].

현대의 시스템은 수많은 구성요소들로 이뤄져 있으며 이에 따라 각각의 구성요소들이 수행하게 되는 기능도 무수히 많다. 더불어 각각의 구성요소들이 개별적으로만 작용하는 것이 아니라 서로간의 인터페이스를 통하여 상호작용하게 된다. 따라서 시스템 수준에서의 위험원 분석이 필요하게 되고 덧붙여 구성요소들의 인터페이스 상에서 발생하는 위험원들에 대한 분석 또한 필요하다[9].

위험원의 분석을 위해 시스템을 분석하는데 있어서 SysML을 활용하여 효과적인 위험원의 분석을 수행 할 수 있다. SysML은 시스템 모델링 언어로써 시스템을 구현할 때 효과를 발휘하는 모델링 언어의 일종이다. SysML은 시스템의 사양화, 분석, 설계, 타당성 확인/검증을 위해 사용 할 수 있고, 현재 자동차, 항공우주, 통신 분야 등에서 광범위하게 활용 되고 있다. SysML은 시스템의 분석 설계 등에 활용하여 시스템을 구현하는데 활용 할 수 있다. 이를 이용하여 기능안전표준에 따라 위험원 분석을 수행하고자 하는 대상 시스템에 대하여 SysML을 활용한 분석을 수행하여 효율적인 위험원 분석을 수행 할 수 있다.



<Figure 2> Procedure model for hazard analysis



<Figure 3> Concept model for current research

시스템의 개발 초기에 가장 먼저 수행하게 되는 PHA(Preliminary Hazard Analysis)의 경우 시스템의 고장 시나리오를 분석하여 위험원을 식별하게 된다. 이때 SysML의 Activity Diagram을 활용하여 대상 시스템에 대한 고장 시나리오 분석을 수행 할 수 있다. 그 다음으로 System Hazard Analysis를 수행하여 대상 시스템의 기능상의 위험원을 식별하게 된다. 이때는 두 가지 방향으로 접근하게 되는데 먼저 식별된 기능에 대하여 Activity Diagram을 통해 거동분석을 하여 기능 수준에서의 위험원 분석을 수행한다. 두 번째로는 구성요소들 간의 인터페이스 상에서 발생 가능한 위험원을 분석하기 위해서 Block Definition Diagram을 활용하여 Interface를 식별하고 이에 대한 위험원 분석을 수행한다.

위험원의 분석은 대상 시스템을 체계적으로 분석하여 얻는 정보가 매우 중요하게 활용되기 때문에 SysML을 활용함으로써 위험원 분석에 이용될 정보들을 효과적으로 얻을 수 있다. 또한 본 연구에서는 시스템의 구성요소들 간의 인터페이스 상에서 발생할 수 있는 위험원의 분석을 수행하고자 하는데 SysML 다이어그램들을 활용하여 대상 시스템을 분석하여 구성요소들 간의 인터페이스의 식별을 수행 할 수 있으며, 이를 바탕으로 인터페이스 위험원의 식별이 가능하다.

복잡성이 증가하고 있는 현재의 시스템에 대하여 요구되는 시스템 수준에서의 위험원 분석을 위해 시스템공학적 측면의 시스템 분석과정이 수행되며 시스템의 분석과정에서 SysML을 활용함으로써 위험원 분석과정에서 활용될 대상 시스템에 대한 분석정보를 획득 할 수 있다.

2.3. 연구 목표 및 범위

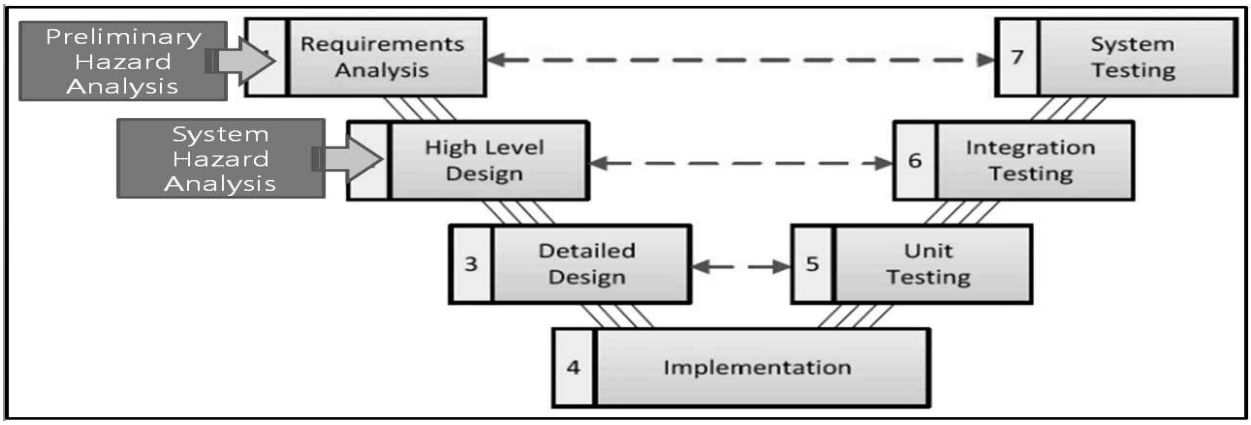
상위 선행연구 분석을 통해 안전 확보를 위한 위험원 분석단계의 중요성에 대해서 인지하였다. 또한 현대의 시스템에 대하여 기능안전표준을 충족시키기에는 재의 위험원 분석 방법으로는 부족함이 있으며 이를 개선 보완하기 위해 기능중심의 위험원 분석 및 SysML의 활용에 대한 필요성에 대해서 제시하였다. 이를 위해 시스템 공학 기반의 위험원 분석의 필요성을 제시하였다. 시스템의 상위수준에서부터 체계적인 위험원 식별을 수행하고 이 때 SysML을 활용하여 대상 시스템을 분석하여 위험원 분석을 수행하는 것이 본 논문의 연구 목표라 할 수 있다.

현재 중요성이 점차 강조되고 있는 기능안전의 달성을 위해 기능중심의 위험원 분석을 수행하기 위해 SysML을 활용하여 시스템을 분석하여 그 결과를 위험원 분석에 활용한다. 이를 바탕으로 구조화된 기능 식별을 통해 개별 기능의 오류로 인한 위험뿐만 아니라 기능간의 상호작용에 의한 위험 또한 식별하여 대응할 수 있도록 한다. 본 논문에서 제시하고 있는 연구 개념은<Figure 3>와 같다.

3. SysML을 활용한 기능중심의 위험원 분석 방법

3.1. 위험원의 유형 및 위험원 분석 방법 분석

위험원 분석을 통해 식별되는 위험원은 두 가지 유형으로 구분 할 수 있다. 개별 구성요소를 통해 도출되는 위험원과 구성요소들 간의 인터페이스 상에서 식별되는 위험원이다. 전자의 경우 대상 시스템을 구조적으로 분석하여 개별 구성요소들을 통해 발생 가능한 위험원을 분석하는 것이다.



<Figure 4> Hazard analysis activities on system development v-model

기능안전표준들에서는 시스템에 대해 기능분석을 수행하여 기능상에서의 위험원의 식별을 수행하도록 제시하고 있다. 후자의 경우엔 복잡성이 증가하고 있는 현대의 시스템에서 중요성이 점차 커지고 있다. 현대의 시스템은 단일 구성요소로 구성된 것이 아니라 다양한 구성요소들이 서로 상호작용하고 있다. 따라서 구성요소들 간의 상호작용을 가능하게 하는 인터페이스 상에서도 위험원이 존재 할 수 있다. 따라서 인터페이스를 분석하여 이에 대한 위험원을 분석하는 것도 중요하다. 이와 같이 두 가지 유형의 위험원이 시스템에 내재하고 있으며 체계적인 시스템의 분석을 통하여 두 가지 유형 모두에 대한 위험원의 분석이 필요하다.

위험원을 분석하고자하는 시스템의 계층, 수명주기에 따른 위험원 분석방법이 안전관련 표준에서 제시되고 있다. <Figure 4>는 시스템 개발에 대한 V-model에 PHA와 SHA(System Hazard Analysis)의 수행시기를 매칭 하여 나타낸 그림이다. 그림과 같이 시스템 설계 초기에 가장 먼저 수행하게 되는 PHA와 이후 시스템 수준에서의 요구사항 및 기능분석 과정에서 수행하게 되는 SHA가 있다.

PHA의 경우 대상 시스템을 운용관점에서 분석하여 고장 시나리오 분석을 수행한다. 시나리오 분석을 통해서 대상 시스템이 운용되는 과정에서 발생 가능한 고장을 분석하여 그에 대한 위험원을 식별하는 과정을 수행하여 위험원 분석을 수행한다. PHA는 시스템 설계의 초기에 시스템의 운용개념이 정해지면 그것을 바탕으로 시나리오를 구성하여 위험원 분석에 활용한다.

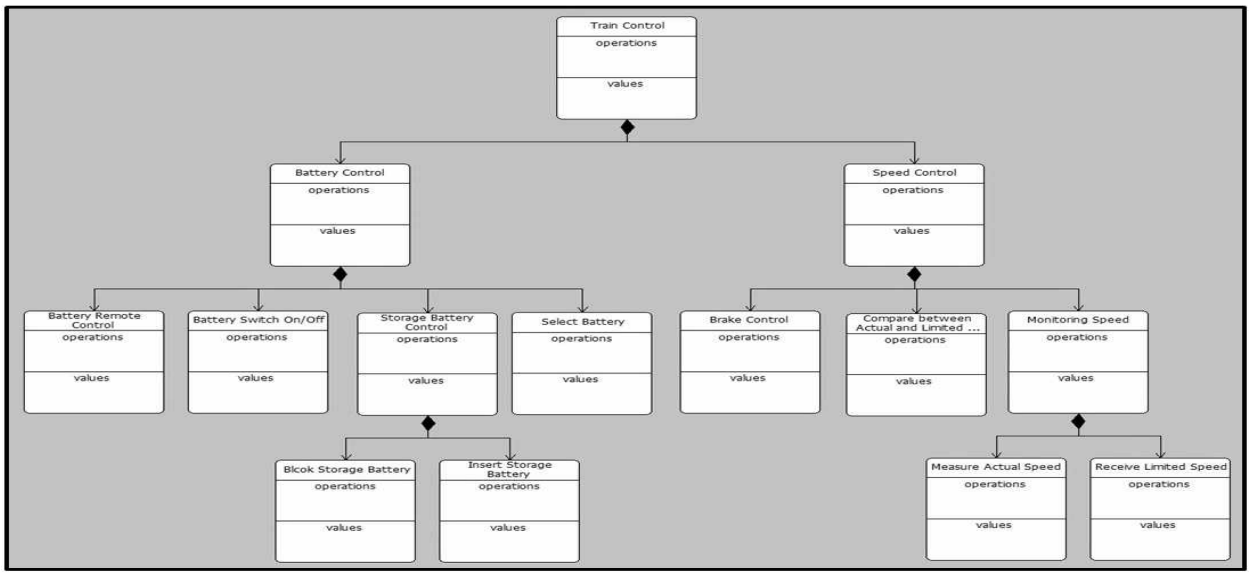
SHA는 시스템의 설계 중 개념설계 단계에서의 요구사항분석, 기능분석 등의 결과를 바탕으로 수행하는 위험원 분석단계이다. 대상 시스템의 대한 정의가 이뤄지면, 시스템에 대한 요구사항 분석, 기능분석이 차례대로 수행하게 된다. 이를 바탕으로 대상 시스템에 대한 구조적인 분석이 가능하여 시스템을 구성하고 있는 구성요소들의 식별이 가능하다. 또한 식별된 구성요소들이 수행하게 되는 기능 또한 식별되며 상위수준의 기능이 하위 수준의 기능으로 분해되어 구성품 수준에서의 기능식별 및 분석까지 이뤄지게 된다. SHA는 식별된 기능들이 제대로 수행되지 않을 경우 발생하게 되는 위험원들을 식별하게 된다. 여기에 덧붙여 상위수준에서 하위수준으로 기능들을 분해하면서 기능들 간의 상호작용에 대해서도 분석이 가능하다. 이를 바탕으로 하여 서로 인터페이스를 가지는 기능들 사이에서 발생 가능한 위험원들 또한 식별이 가능하다.

이와 같이 시스템 설계 초기 단계부터 PHA, SHA를 수행함으로써 미리 위험원의 식별이 분석이 이뤄지게 되면, 향후 설계 과정 및 운용단계에서 발생 가능한 고장 및 오류에 대한 대응을 적절하게 수행할 수 있게 된다.

3.2. SysML을 활용한 PHA 및 SHA의 수행

앞 절에서 언급했듯이 PHA와 SHA는 시스템의 개발초기부터 수행되어야 할 위험원 분석 절차이다. 또한 적절한 PHA와 SHA를 수행하기 위해서는 대상 시스템에 대한 체계적인 분석이 필요하다. 개념설계 단계에서의 요구사항 분석과 기능분석을 통하여 PHA와 SHA의 수행이 가능하다.

개념설계 단계에서의 요구사항 분석과 기능분석을 통한 위험원 분석의 첫 단계로 사용자의 needs로부터 요구사항을 도출한다. 그 후 도출된 요구사항을 구현하기 위한 기능들을 식별한다. 마지막으로 식별된 기능이 오류를 일으킴으로 발생 할 수 있는 고장들을 식별한다. 이는 단순히 장치 부품수준에서 개별 장치 및 부품에 대한 고장이 아닌 시스템 수준에서 분석된 고장이라 할 수 있다.



<Figure 5> Block definition diagram of train control system

SysML은 여기서 효과적인 기능분석을 수행하기 위해 활용된다. 본 연구에서는 SysML의 여러 Diagram들 중 Activity Diagram과 Block Definition Diagram을 활용하여 기능분석을 수행 하였다. Block Definition Diagram은 Block과 Block간 관계를 정의하기 위한 Diagram이다[10]. 이는 기능분석을 수행하기 전에 대상 시스템에 대한 정의를 명확히 하는 과정에서 활용하였다. 대상 시스템을 Block Definition Diagram으로 분석함으로써 대상 시스템의 구성요소와 구성요소간의 관계를 식별할 수 있다. 또한 Block Definition Diagram을 활용하여 기능들 간의 Interface를 분석하여 인터페이스 상에서 발생 할 수 있는 위험원에 대해서도 분석이 가능하다. 즉 Block Definition Diagram은 위험원 분석을 수행하기 위한 시스템의 정의과정과 SHA의 수행과정에서 Interface의 분석에 활용하였다.

Activity Diagram은 작업이나 처리가 어떤 순서로 진행되는지, 또한 어떤 조건에서 처리가 실행되는지에 대해서 시스템이나 그 구성요소의 Behavior를 표현하기 위한 Diagram이다[10].

본 연구에서는 Activity Diagram을 기능분석에 활용하였다. 요구사항을 바탕으로 기능들을 식별한 후에 기능들의 순서와 상호 관계 등을 포함하는 기능에 대한 거동분석을 하는데 Activity Diagram을 활용 하였다. 이는 기능안전표준에서 지향하는 기능중심의 위험원 분석을 보다 체계적으로 수행 할 수 있도록 해준다. Activity Diagram을 통해 개별 기능의 식별만이 아니라 기능들 간의 관계를 파악하여 시스템 수준에서의 위험원 분석이 가능하게 해준다.

또한 Activity Diagram을 통해서 시스템의 시나리오를 분석하였다. 이는 시스템의 개발초기에 PHA를 수행하기 위함으로써 Activity Diagram을 활용한 시나리오 분석을 통해 시스템의 운용상에서 발생 가능한 위험원의 분석이 가능하다. 즉 Activity Diagram은 PHA를 수행하기 위한 시나리오 분석과 SHA를 수행하기 위한 거동분석에 활용하였다.

이와 같이 SysML에서 지원하는 여러 Diagram을 시스템의 분석에 활용함으로써 그 결과를 바탕으로 PHA와 SHA를 수행하였다.

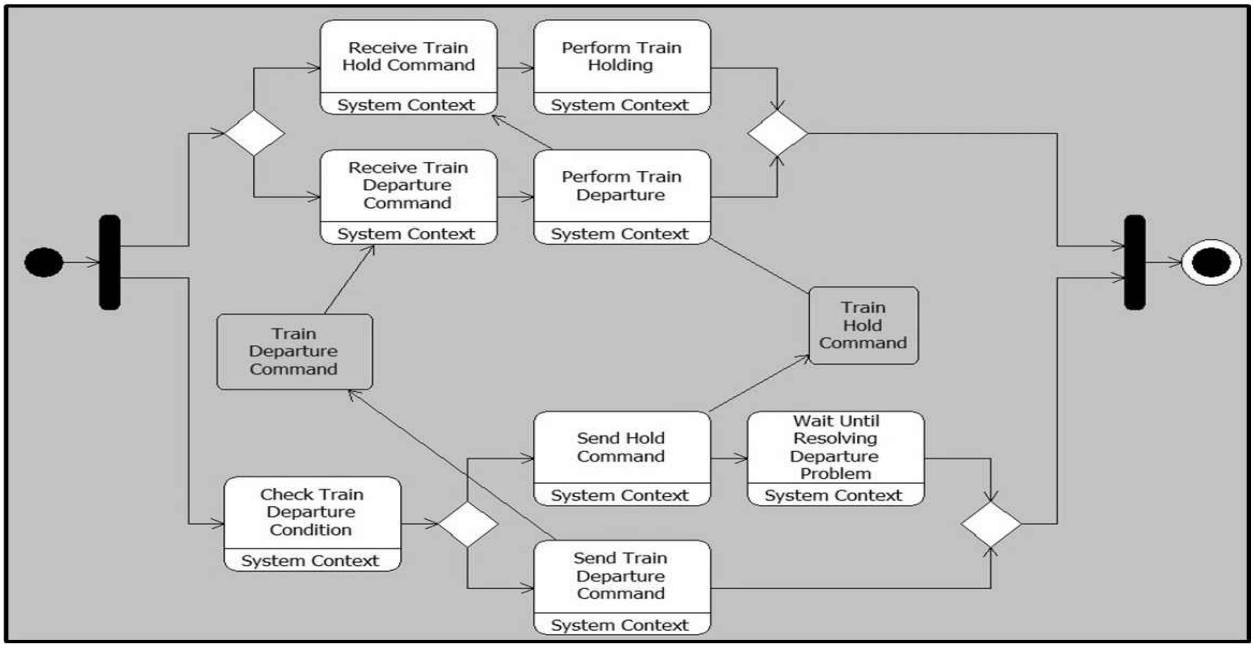
4. SysML을 활용한 철도 시스템의 위험원 분석

3장에서 제시한 SysML을 활용한 위험원 분석방법에 따라 철도시스템에 대한 위험원 분석을 수행했다. 먼저 시스템 정의를 통해 대상시스템의 요소를 식별하였다. 다음으로 기능분석을 통한 철도차량 운전실 위험원 식별을 수행했다. 이를 통해 기능안전표준에서 지향하는 기능중심의 위험원 식별을 달성했다. 그 결과를 1,2절에 제시하였다.

4.1. 시스템 정의

철도시스템은 철도차량, 철도 인프라, 신호 및 제어시스템 등을 포함하는 복합 시스템이라 할 수 있다.

철도 시스템에서 철도 신호 및 제어시스템은 철도 차량을 운행하는 과정에서 인명 사상 및 시설물 파손 등의 사고가 발생하는 것을 방지하는 시스템이라 할 수 있다.

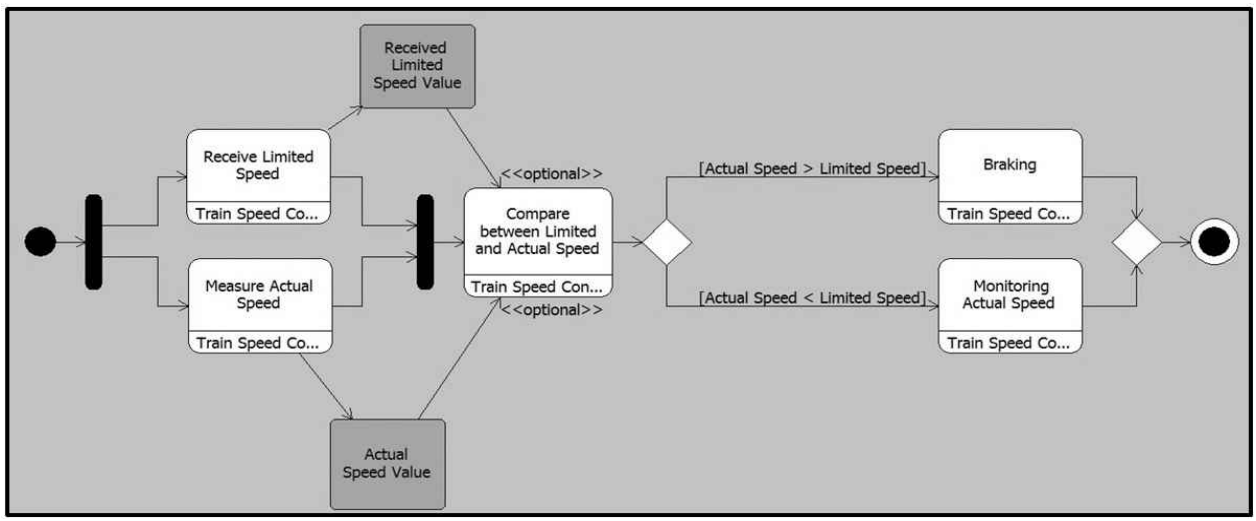


<Figure 6> Activity diagram of train start

철도 제어 시스템을 구축, 운용하기 위해서는 철도운행과정에서 발생할 수 있는 위험원 식별, 위험 대책 설계 및 안전성 확인, 검증과 같은 위험원 분석 활동이 반드시 필요하다. 이에 더하여 철도 제어시스템에서 소프트웨어, 유, 무선통신기술등의 비중이 증가함으로써 위험원 분석을 포함하는 안전성의 확보가 더욱 중요해졌다.

철도 선진국에서는 IEC 61508 기능안전표준을 바탕으로 하여 철도분야에 적용한 IEC 62278, 62279, EN 50126, 50128, 50129 등의 철도 및 철도 신호, 제어시스템에 대한 기능안전표준을 제정하여 철도 제어 시스템에 대한 정의 및 안전성을 확보하기 위한 안전관리 활동에 대해 정의 하고 있다.

철도 제어시스템은 철도차량의 안전한 운영을 위한 배터리 제어, 속도 제어, 통신 제어 등 다양한 차량 제어부로 구성이 되어있다. <Figure 5>는
차량 제어시스템에 대한 Block Definition Diagram의 일부이다. 차량 제어중 배터리 제어와 차량 속도 제어 및 그 하부 구성요소에 대해 식별하였다. 이를 활용하여 SHA를 수행하는데 있어서 대상 시스템을 구조적으로 파악하고 구성요소간의 관계를 파악하여 위험원의 분석을 수행 하였다.



<Figure 7> Activity diagram of train speed control

[Table 1] Result of identifying hazards on train start

Category of train start control function	Hazard	Deviation
to transmit train start/stop signal to command center	Impossible to transmit signal	Trains cannot start since it is not possible to transmit train start/stop signals to command center.
	Wrong signal transmitted	Trains cannot start since wrong signals for train start/stop are transmitted to command control center.
to confirm train start condition	Impossible to monitor train status	Trains cannot start since it is not possible to monitor train status.
	Impossible for train and command control center to communicate between them	Trains cannot start since it is not possible for train and command control center to communicate between them.
to receive train control command	Wrong control command received	Trains cannot start since wrong control command is received.
	Impossible to receive train control command	Trains cannot start since it is not possible to receive train control command.

4.2. SysML을 활용한 철도시스템에 대한 PHA 및 SHA 수행

4.1절에서 정의한 철도 제어시스템의 대한 정의를 바탕으로 철도 제어시스템에 대한 위험원 분석을 수행하였다. 이를 위해 철도 제어에 대한 Activity Diagram을 모델링 했다. 먼저 <Figure 6>와 같이 철도차량의 운행을 시작할 때의 제어에 대하여 Activity Diagram을 구현했다. 이를 바탕으로 하여 철도차량을 출발할 때의 시나리오를 파악할 수 있다.

<Figure 6>를 보면 차량의 운행을 시작하는 데에는 차량에 있는 제어부와 차량에 제어 신호를 보내주는 관제부가 제어를 수행함을 알 수 있다. 차량의 출반 조건을 확인하여 관제부에서 차량 출발 또는 정지 신호를 차량으로 전달하면 차량에서는 신호를 전달받아 신호에 따른 차량 제어를 수행하게 된다.

Activity Diagram에서 식별된 차량 출발에 대한 신호를 바탕으로 하여 차량 시작을 위한 제어기능들과 신호를 주고받는 과정에서 발생 가능한 위험원들을 식별 하였다.

다음으로 철도 시스템이 출발한 후의 차량 속도제어에 관한 Activity Diagram을 모델링 했다. <Figure 7> 속도 제어에 관한 Activity Diagram을 분석하면 차량의 속도 제어를 위해서는 먼저 관제부로부터 현재 달리고 있는 선로에서의 제한속도 값을 전송받는다. 이후 현제 운행되고 있는 차량에 대한 실제 속도를 지속적으로 측정한다. 그 후 전송받은 제한 속도 값과 현재 측정되고 있는 실제 차량 속도 값 을 지속적으로 비교하며 비교한 결과가 현재 속도가 제한속도 값보다 높을 경우 브레이킹을 수행하고 제한 속도 값 보다 낮을 경우엔 지속적으로 현재 운행속도에 대한 모니터링을 수행한다.

Activity Diagram을 바탕으로 해서 차량의 속도제어에 수행되는 하부 기능들에서 발생 가능한 위험원에 대하여 식별하였고, 관제부와의 데이터 전송과정에서 발생 가능한 위험원도 식별하였다.

SysML의 Activity Diagram 및 Block Definition Diagram을 활용한 위험원 분석 결과의 일부를 <Table 1>, <Table 2>에 정리했다.

<Table 1>은 철도차량의 출발 제어 시에 발생하는 위험원에 대하여 식별한 것이다. 차량의 출발제어에 수행되는 기능들을 식별하고 기능상에서의 위험원 식별하였고 이로 인해 발생 가능한 위험에 대하여 Deviation으로 식별하였고, 그 결과를 Hazard List에 작성했다. 이를 기반으로 차량 출발제어 시에 기능오류로 인해 발생 가능한 위험원을 식별하였고, 향후 이에 대한 대응책을 구성함으로써 위험에 대비 할 수 있다.

<Table 2>는 차량 운행 중 속도 제어에 대한 위험원을 분석한 결과 이다. 속도 제어를 위해 필요한 기능에는 실제 차량 운행속도 측정, 차량 운행속도와 제한속도 비교, 관제부와의 속도 값 송수신 기능 등이 필요하다. 식별된 기능들에서 발생 가능한 위험원들을 식별하였고, 이로 인해 발생 가능한 위험에 대하여 Deviation으로 식별하여 Hazard List를 작성했다.

[Table 2] Result of identifying hazards on speed control

Category of train velocity control function	Hazard	Deviation
to measure actual velocity	Impossible to measure velocity	The speed of the train cannot be controlled since it is not possible to measure the velocity of the running train.
	Incorrect velocity measure	The speed of the train cannot be controlled due to incorrect velocity measures.
to compare actual velocity and limit velocity	Incorrect comparison result	The speed of the train cannot be controlled since the comparison of actual velocity and limit velocity is incorrect.
	Impossible to compare velocities	The speed of the train cannot be controlled since it is not possible to compare actual velocity and limit velocity.
to exchange velocity values with command control center	Impossible to transmit velocity value to command control center	The speed of the train cannot be controlled since it is not possible to exchange velocity values with command control.
	Erroneous limited velocity received	The speed of the train cannot be controlled due to erroneous limited velocity received.

시스템을 분석하는 과정에서 SysML Diagram을 활용하였고 그 결과를 기능분석 및 시나리오 분석에 활용하여 시스템의 위험원을 분석했다. 이는 기존의 위험원 식별 기법들인 FMEA나 HAZOP등이 하위 수준에서 부터의 위험원 분석인 것과는 달리 상위수준에서부터의 체계적인 시스템 분석 과정의 결과로써 얻어진 위험원 분석결과 이다.

시스템을 정의하고 시스템에 대한 요구사항을 식별하고 요구사항을 충족시키기 위한 기능을 식별한 후 이에 대해 SysML을 활용한 모델링을 통해 거동분석을 수행함으로써 기능안전표준에서 명시하고 있는 기능중심의 위험원 분석이 가능하다. 또한 SysML을 활용함으로써 개별 기능뿐만 아니라 기능간의 관계에 대해서도 분석이 가능함으로써 인터페이스 상에서 발생 가능한 위험원도 식별 가능 하다.

5. 결 론

오늘날 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 철도와 같은 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 따라서 체계적인 안전관리의 필요성이 점차 커지고 있다.

더불어 시스템에서 전기, 전자 장치 및 소프트웨어의 비중이 높아짐에 따라 기능안전의 중요성이 높아지고 있다. 이에 따라 IEC 61508, ISO 26262, IEC62279 등의 기능안전 표준들이 제정되어 산업에 적용되고 있다.

본 논문에서는 대상 시스템에 대한 안전을 확보하기 위해 기능안전표준에서 명시하고 있는 기능중심의 위험원 분석방법에 대한 연구를 수행하였다. 기능중심의 위험원 분석을 위해 시스템을 분석하는 과정에서 SysML을 활용한 모델링 결과를 활용했다.

기능 분석과정에서 SysML을 활용함으로써 개별 기능에 대한 위험원뿐만이 아니라 기능간의 인터페이스 상에서 발생 가능한 위험원들 또한 식별이 가능하였다. 이를 통해 기능안전표준에서 제시하고 있는 시스템 수준에서의 기능안전의 달성이 가능하다.

시스템은 단일 기능으로 구성된 것이 아니라 다양한 기능이 포함되어 있고, 이들 기능간의 무수한 상호작용으로 시스템의 운용이 된다. 따라서 개별 기능에 대한 위험원 분석뿐만이 아니라 기능들 간의 인터페이스 상에서의 위험원 분석의 중요성이 커지고 있으며 본 연구에서는 이를 SysML Diagram을 활용하여 수행하였다.

이는 기존의 위험원 분석 방법이 부품 장치수준에서부터 이뤄졌고, 또한 개별 구성품 들에 대한 위험원 분석이었다는 단점을 보완한 것이며, ISO 61508을 바탕으로 한 기능안전표준들에서 상세히 제시하고 있지 않은 시스템 수준의 기능안전을 구현하는 방법으로 제시될 수 있다.

기능안전규격들은 기능안전의 달성을 위해 위험원 분석을 수행하라고 제시하고 있지만 상세한 방법론은 제시하지 않고 있다. 본 논문에서 제시하고 있는 SysML을 활용한 기능 중심의 위험원 분석을 통해 기능 안전 규격에서의 기능안전을 달성 할 수 있다. 향후 기능 중심의 위험평가 까지를 고려하여 시스템 수준에서의 기능 중심의 위험원 분석 전체 활동을 수행 하는 것에 대한 연구를 수행 할 필요가 있다.

6. References

[1] Marco de Bruin, Paul Swuste, (2008), "Analysis of hazard scenarios for a research environment in an oil and gas exploration and production company.", Safety Science, 46: 261-271

[2] Maddalena Casamirra, Francesco Castiglia, Mariarosa Giardina, C. Lombardo, (2009), "Safety studies of a hydrogen refuelling station: Determination of the occurrence frequency of the accidental scenarios.", International Journal of Hydrogen Energy, 34: 5846-5854

[3] Y.M. Chen, K. S. Fan, and L. C. Chen, (2010), "Requirements and Functional Analysis of a Multi-Hazard Disaster-Risk Analysis.", Human and Ecological Risk Assessment : An International Journal, 16: 413-428

[4] Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission Standard, IEC 61508, 2010.

[5] Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS), International Electrotechnical Commission Standard, IEC 62278, 2002.

[6] Road vehicles Functional safety , International Organization for Standardization Standard, ISO 26262, 2011.

[7] Jordi Dunjo, Vasilis Fthenakis, Juan Vilchez, Josep Arnaldos, (2010), "Hazard and Operability (HAZOP) analysis. A literature review.", Journal of Hazardous Materials, 173: 19-32

[8] Rob Alexander, Tim Kelly, (2013), "Supporting systems of systems hazard analysis using multi-agent simulation.", Safety Science, 51: 302-318

[9] Patrick Redmond, (2007), "A system of systems interface hazard analysis techniques," M.S. thesis Naval Postgraduate School, Monterey, CA

[10] OMG System Modeling Language, (2012), Object Management Group Standard

저 자 소 개

정 호 전

현 아주대학교 시스템공학과 박사과정. 관심분야는 시스템 안전 관리체계, 위험원 분석 및 식별, 모델기반 시스템공학, Modeling & Simulation 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 244호

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사 학위를 취득. 미국 MIT (Massachusetts Institute of Technology)에서 Post-Doc을 수행하였으며, 미국 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, 모델기반 시스템공학 (MBSE), Systems Safety, Systems T&E 및 다양한 산업 분야에서의 응용 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호