Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 11 pp. 574-582, 2018

https://doi.org/10.5762/KAIS.2018.19.11.574
ISSN 1975-4701 / eISSN 2288-4688

SysML 기반 모델링 및 시뮬레이션 기법을 통한 기능안전 설계 대안들의 평가 및 결정 방법

정호전, 이재천*
아주대학교 시스템공학과

Evaluation and Determination of System Design Alternatives Utilizing a SysML-Based M&S Method for Achieving Functional Safety

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

요 약 철도, 자동차, 항공 등의 시스템에서는 시스템의 고장이 사고로 이어져 심각한 인명피해와 경제적 손실로 직결되는 경우가 많기 때문에 시스템 안전의 확보가 매우 중요하다. 기존 연구들에서는 구성품 수준의 정보를 활용해서 고장 분석 및 안전조치를 도출하고 이를 통해 고장이 발생했을 때 피해를 경감시키기 위한 안전설계가 주로 수행되었다. 그러나 기능안전 개념에 의한 설계는 위험원 식별 및 평가 그리고 안전기능을 생성한 후 안전 설계를 통해 안전 목표를 달성하고자 하는 것이다. 따라서 시스템의 기능수준에서 고장의 현재 빈도를 수용 가능한 목표수준으로 빈도를 낮출 수 있는 안전기능을 결정하고 이를 설계에 반영하기 위한 방법에 대한 연구가 필요하다. 이를 달성하기 위하여 본 연구에서는 먼저 시스템모델링 언어인 SysML을 활용하여 안전기능 들에 대해 고장빈도를 반영하기 위한 고장 모델링 방법을 연구하였다. 그리고 나서 생성된 SysML 고장모델 대안들의 시뮬레이션을 통해 각 안전기능 들이 달성할 수 있는 고장빈도의 감축능력을 평가해서 안전목표를 충족하는 대안을 결정하는 방법을 제시하였다. 사례 연구로서 대표적인 안전중시 시스템인 철도신호시스템에 적용하여 유용성을 확인하였다. 철도신호시스템의 안전기능 형태의 설계 대안들에 대해 안전 목표를 충족하는 지를 M&S를 통해 비교평가 하였다. 본 연구의 결과는 시스템의 개념설계 단계에서부터 적용 가능한 방법으로 안전기능을 수행하기 위한 다양한 설계대안 들 중에서 적절한 것을 선택함으로써 안전 목표를 충족하는 시스템의 안전 설계에 유용하게 활용될 수 있을 것이다.

Abstract In systems such as railways, automobiles, and airplanes, system malfunctions may lead to accidents, which often cause serious personal injury and economic loss. In previous studies, failure analysis has been performed, and safety measures derived using the component level information to reduce damage when a failure occurs. However, in functional safety concept, a focus is placed on lowering the frequency of occurrence of failures by performing risks analysis, setting up safety goals, and designing safety functions. Therefore, it is necessary to study how to determine the required safety function that can reduce the failure frequency to the acceptable level. To achieve this, we first studied a failure modeling method using SysML. It was then presented how several alternatives can be assessed to determine the desired safety function by simulating the generated SysML failure models and calculating the ability to reduce the failure frequency. A case study of a railway signaling system was done, demonstrating the effectiveness of the approach. We assessed whether the safety objectives were met for the alternative design of the railway signaling system through M & S. The results can be useful in that it can be applied from the early design phase and allow to choose the appropriate safety function that satisfies safety objectives among various design alternatives.

Keywords : Design Alternative Evaluation, Railway Signaling System, Safety Analysis, Safety Design, SysML based M&S

본 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01056730)
*Corresponding Author : Jae-Chon Lee(Ajou Univ.)
Tel: +82-31-219-3941 email: jaelee@ajou.ac.kr
Received August 10, 2018 Revised (1st August 31, 2018, 2nd September 4, 2018)
Accepted November 2, 2018 Published November 30, 2018

1. 서론

IEC 61508로 대표되는 기능안전 표준에서는 안전 중시 시스템에 대해 설계단계에서부터 안전을 확보하기 위한 절차를 제시하고 있다. 표준의 절차에서는 설계단계에서 위험원을 식별하고 평가하며, 위험원에 대한 안전조치를 안전기능의 형태로 식별하여 설계에 반영하는 것 등을 포함하고 있다. 이를 통해 시스템의 설계단계에서부터 안전의 확보가 가능해진다[1]. 이때 시스템이 안전목표를 충족 할 수 있도록 정의하는 안전기능은 위험원에 대해 단일한 것이 아닌 다양한 방안들이 도출 될 수 있다. 기능 수준에서 안전기능이 어떤 형태로 반영될지, 구성품 수준에서 안전기능이 어떤 형태로 구현될지 등에 대해 설계과정에서 결정이 이뤄져야 한다[2]. 따라서 여러 설계 대안들에 대해 안전 목표, 성능들을 충족하는지에 대해 분석하는 것이 필요하다. 이와 관련하여 Modeling&Simulation(이하 M&S)을 활용하여 대안분석을 하는 연구들이 수행되고 있다. 기존연구에서는 구성품 수준에서 안전조치가 반영된 모델을 생성하여 분석하였다. 이 경우에는 기능수준에서 안전기능을 식별하고 구성품 수준에서 구현 한 것이 아니라 구성품 수준에서 safety device 형태의 안전조치들을 이미 결정하여 반영한 케이스이다[3-6]. 이러한 방법은 유사 시스템에 대해 쉽게 안전조치들을 반영한 설계를 수행 할 수 있다는 장점이 있다. 하지만 복잡성이 증가하고 있는 현대의 시스템에 대해서는 다양한 형태의 안전조치를 분석 평가하여 결정하는 것이 필요하다. 따라서 본 논문에서는 기능 수준에서는 다양한 안전기능을 식별하고 이것이 구성품 수준에서 구현이 되었을 때 안전 목표를 충족하는지를 평가하는 방법을 M&S 기반으로 제안하였다. 이를 통해 설계 대안들 중 목표로 하는 안전수준을 효율적으로 달성 할 수 있는 설계 대안을 결정 할 수 있다.

본 논문의 구성은 다음과 같다. 서론에서는 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 M&S 기반의 안전 목표를 고려한 설계대안 평가방법을 제안하였다. 4장에서는 3장의 방법을 활용하여 철도 신호시스템에서 설계대안 평가를 수행한 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 문제 정의

2.1 안전표준 기반의 안전 분석 절차 분석

시스템의 안전을 확보하기 위해 다양한 안전표준이 제정되어 활용되고 있다. IEC 61508을 모 표준으로 하여 철도분야에서는 IEC 62278 자동차 분야의 ISO26262, 공정분야의 IEC 61511등의 표준이 제정되어 각 분야에서의 수행되어야 할 안전 분석 절차가 제시되어 있다. 또한 표준에서는 시스템의 설계와 연계하여 안전 분석 활동이 수행되어야 함을 제시하고 있다[2, 7-9]. 여러 안전표준에서 제시하고 있는 안전 분석 절차는 Fig. 1과 같다.

먼저 대상 시스템에 존재하고 있는 위험원을 식별한다. 그 후 식별된 위험원에 대한 리스크를 평가하여 리스크 관리가 필요한 위험원들을 선정한다. 그 후 관리가 필요한 위험원들에 대한 리스크 경감 대책을 수립한다. 이때 안전기능 형태의 안전조치들이 식별된다. 안전기능이 식별되는 이것을 설계에 반영하여 안전을 확보 할 수 있도록 한다. 여러 산업분야에서 Fig. 1과 유사한 절차를 따르고 있으며 세부적인 방법들을 각 분야에 맞게 제시하고 있다. 이와 같이 많은 산업분야에서는 설계 단계에서부터 안전을 확보하기 위한 절차를 표준들을 통해 제시하고 있다.

2.2 기존의 안전분석 절차에서 설계대안 평가 방법 분석

2.1에서의 안전분석 절차를 따라 안전분석 활동을 수행하게 되면 관리가 필요한 위험원에 대한 안전조치를 식별하게 된다. 그 후 안전 조치를 설계에 반영하는 것은 안전설계라 지칭한다. 이때 기존에는 구성품 수준에서 안전조치를 결정하는 경우가 많았다.

Fig. 1. Safety Analysis Process

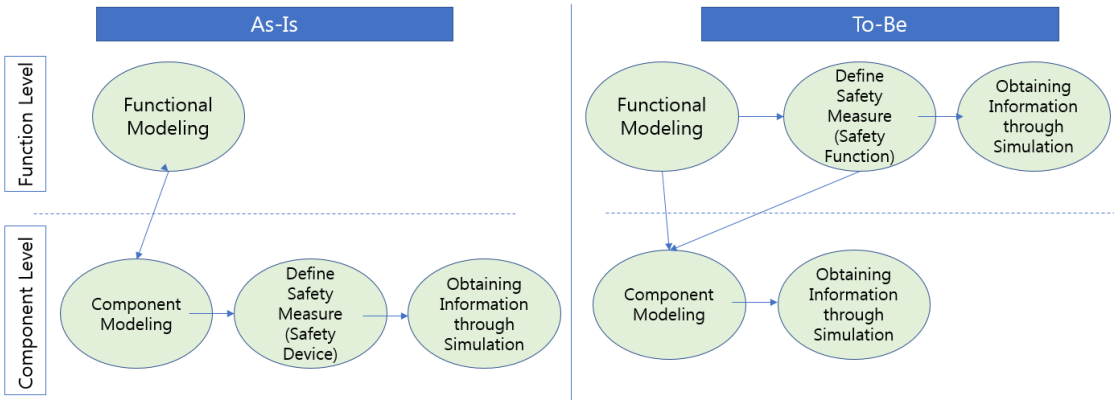

Fig. 2. Concept of M&S based Alternative Assessment: Existing and Proposed

Ordouei 등[11]은 화학공정분야에서의 두 가지 안전 조치를 반영한 설계 대안을 비교 평가하는 연구를 수행하였다. 이때의 두 가지 안전 조치는 밸브의 형태로 안전 기능을 식별하여 도출한 것이 아닌 사고 발생 시 피해를 최소화하기 위한 safety device로써 밸브를 두 가지 형태로 설계에 반영하였다. 그리고 이 두 가지 설계에 대해 리스크 및 생산량을 평가하여 리스크 감소와, 생산량 측면에서 더 이득이 있는 설계 대안을 결정하는 방법을 제안하였다.

Kurtoglu 등[12]은 전력시스템의 일부 서브시스템에 대하여 리스크를 경감하는 두 가지의 설계 대안을 도출하여 서로 비교 평가하는 방법을 제안하였다. 전력시스템의 구성품수준의 설계정보를 활용하여 구성품수준에서 안전조치가 반영되었을 때 리스크가 경감되는 것을 비교 평가하는 방법을 제안하였다.

Cambell 등[13]은 기계분야에서 시스템의 구성품 설계 정보를 바탕으로 역으로 기능모델을 도출하여, 기능수준에서 설계 대안들을 비교 평가하는 방법을 제안하였다.

이와 같이 안전을 고려한 설계대안 평가방법이 연구되고 있지만 이때 설계 대안들을 생성하는 안전조치는 대부분 safety device를 부착하는 형태이다. 구성품수준에서 적용되는 안전조치들이라 할 수 있다. 이는 고장의 빈도를 줄이는 것이 아닌 고장이 발생했을 때 피해를 줄이는 형태이다. 최근의 안전은 active safety라 하여 고장의 발생빈도 자체를 줄이는 방향으로 안전을 확보한다. 고장의 피해를 줄이는 것은 passive safety라 화여 과거에 주로 활용되던 안전확보 방법이다. 따라서 기존의 구성품 수준에서 안전조치를 결정하고 이를 반영한 모델을 만들어 설계 대안들을 비교하는 것은 과거의 passive safety를 충족시키는 형태라 할 수 있다. 이것은 유사 시스템에 활용되었던 safety device들을 쉽게 활용할 수 있는 장점이 있지만, 점점 복잡해지고 있고 한번 고장으로 인한 사고가 발생하면 큰 피해를 유발할 수 있는 현대의 시스템에 있어 온전히 안전을 확보하기에는 부족한 점이 있다. 설계단계에서부터 고장의 원인을 분석하여 이것의 빈도자체를 줄이는 설계의 필요성이 증대되고 있다. 이것이 최근 제정되고 있는 안전표준을 충족하는 안전설계라 할 수 있다.

2.3 M&S 기반 설계대안 평가방법의 개선 필요성

2.2절에서 분석하였듯이 안전을 고려한 설계대안 평가방법들이 연구되고 있다. 하지만 대부분 물리적 구성품 수준에서 적용 가능한 안전조치들을 통해 설계 대안들이 생성되었다. 따라서 안전조치에 의한 리스크의 경감을 비교 평가하는 것도 구성품 수준에서의 모델링과 시뮬레이션을 활용하여 수행되었다. 이는 2.2절에서 분석하였듯이 passive safety 형태의 안전조치와 이를 통한 리스크의 경감을 비교 평가하는 방법이다. IEC 61508등을 비롯한 안전표준에서는 기능 수준에서 안전기능을 식별하여 설계에 반영하여 고장의 발생빈도 자체를 경감시키는 active safety 형태의 안전설계를 권장하고 있다. 따라서 기능수준에서 안전기능이 반영되는 설계 대안들을 생성하고 이에 대해 리스크 경감 수준을 빈도 기반으로 평가하는 방법이 필요하다. Fig. 2는 기존의 M&S 기반 설계대안 평가 방법과 본 논문에서 제안하는 방법을 나

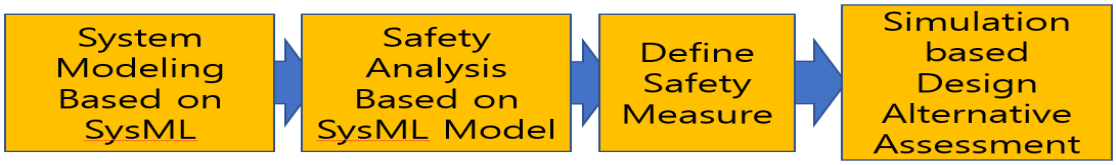

Fig. 3. Concept Model for Current Research

타낸 것이다. 기존에는 안전조치도 구성품 수준에서 적용되던 방법이고 리스크의 평가도 구성품 수준을 중심으로 이뤄졌다. 본 논문에서는 기능 수준에서 안전기능의 형태로 안전 조치를 식별하고 이에 대한 리스크 평가도 기능 수준에서 수행한다. 그리고 안전기능이 구성품 수준의 설계에 반영되면 이때는 비용, 성능 등의 평가를 수행 하여 적절한 설계 대안을 결정할 수 있을 것이다.

2.4 연구목표 및 범위

선행연구 분석을 통해 기존의 구성품 중심으로 수행되던 설계대안 평가를 기능수준에서 수행해야 할 필요성과 이에 대한 수행방법의 필요성이 인지되었다. 따라서 본 논문에서는 기능 수준에서 기능모델 및 시뮬레이션을 통해 설계 대안을 비교 평가하는 방법을 제안하는 것을 목표로 한다.

Fig. 3은 본 논문의 연구 수행 절차이다.

본 논문에서의 설계대안 평가 절차는 (1) 분석대상이 되는 시스템의 설계정보를 모델링 하는 것. (2) 모델링된 설계정보를 기반으로 안전 분석을 수행하는 것. (3) 안전분석 결과를 활용하여 다양한 안전조치를 식별하고 이를 모델에 다시 반영하는 것. (4) 안전조치가 반영된 대안 모델을 활용하여 안전목표 및 설계목표를 충족하는 대안을 시뮬레이션을 통해 결정하는 것까지를 포함하는 절차이다.

위의 절차에 따른 설계 대안을 평가하는데 SysML 기반의 M&S를 활용하는 방법을 본 논문에서 제안한다. SysML은 대표적인 시스템 모델링 언어로써 대상 시스템의 설계정보를 모델링 할 수 있다[14]. SysML기반의 시스템 모델링, 안전조치가 반영된 설계대안의 생성, 대안들을 SysML 시뮬레이션을 통한 빈도측면의 리스크

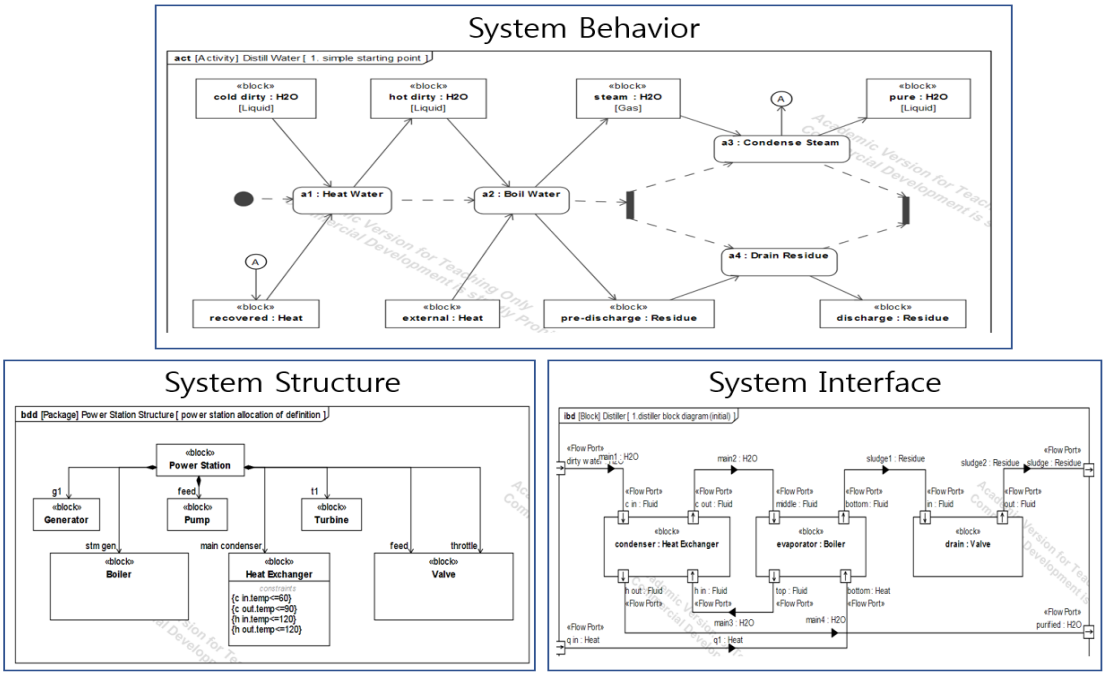

Fig. 4. SysML based System Modeling Concept

평가 등을 수행하는 방법을 제안하는 것이 본 논문의 연구 범위이다.

3. 설계대안 평가를 위한 SysML 기반 M&S 수행 방법

3.1 SysML기반의 대상 시스템 모델링

M&S 기반의 설계 대안 평가를 위해선 대상 시스템의 모델링이 우선적으로 수행된다. 대상 시스템의 설계 정보를 기반으로 기능, 구성품 수준의 모델링 수행하여 대상 시스템의 안전 분석을 수행하는 정보로 활용한다. 본 논문에서는 대표적인 시스템 모델링 언어인 SysML을 활용하여 대상 시스템을 모델링한다. Fig. 4는 SysML을 활용한 대상 시스템의 모델링 방법을 보여준다. SysML모델링을 통해 대상 시스템의 구조, 거동, 인터페이스의 분석이 가능하다. Fig. 4와 같이 Block Definition Diagram(이하 BDD)을 통해 대상 시스템, 기능, 구성품에 대한 구조를 분석 한다. Activity Diagram을 통해서는 기능의 거동을 분석 한다. 기능들의 수행 순서, 기능간의 인터페이스의 분석을 수행한다.

Internal Block Definition Diagram은 구성품간의 인터페이스를 분석 한다. 이와 같이 SysML모델을 통해 대상 시스템의 안전 분석에 필요한 대상의 구조, 거동, 인터페이스 정보를 획득 할 수 있다.

3.2 모델링 결과를 활용한 설계대안 평가를 위한 정보 도출

3.1절에서 수행한 모델링 결과를 통해 안전 분석에 필요한 정보를 분석, 획득 할 수 있다. Fig. 5 는 SysML모델의 정보와 안전 분석 활동 간의 관계를 식별하여 도출한 것이다. 안전 분석 각 단계에서 필요한 설계정보를 SysML모델링 결과로부터 확보 할 수 있다. 위험원 식별 단계에서 위험원 식별의 대상을 BDD에서 결정 한다. 또한 BDD를 통해 확보한 기능, 구성품들의 계층구조는 위험원 분석을 수행 할 때 상, 하위 계층 간의 연계성에 관

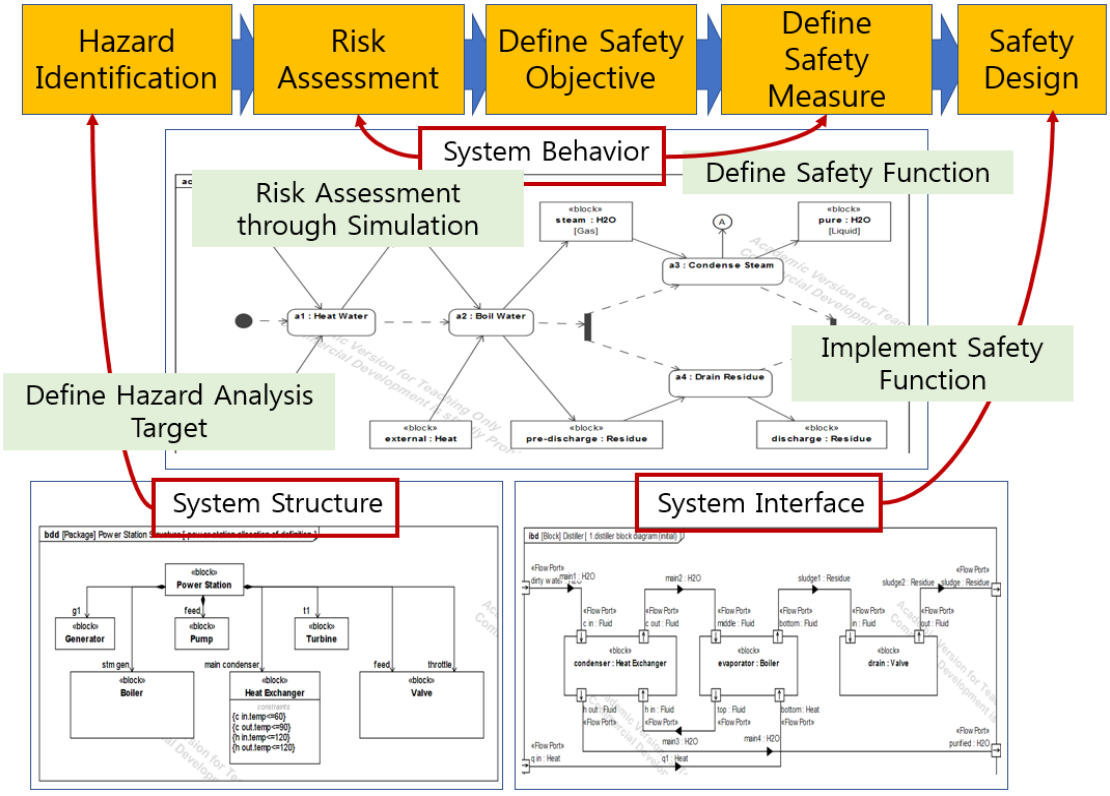

Fig. 5. Relationship between SysML based System Model and Safety Analysis

한 정보를 제공해준다. 하위 구성요소의 위험원이 시스템 수준까지 어떻게 영향을 미치는지에 대해 계층구조를 활용하여 분석을 수행해야 한다.

위험원 평가 및 안전기능의 식별 단계에서는 Activity Diagram기반의 거동분석을 활용한다. 기능에 대한 위험원을 식별 한 후 하나의 기능의 고장이 다른 어떤 기능에 영향을 미치는 지를 거동분석 결과를 활용하여 식별한다. 또한 기능고장에 대한 안전 기능을 식별하였을 때 Activity Diagram상에서 어떤 형태로 안전 기능이 작동하는지를 미리 분석하여 결정해야 한다. 그 후 안전기능 반영 전후의 Activity Diagram을 시뮬레이션 하여 반영 전후의 고장 발생 빈도를 평가한다. 이를 통해 여러 설계 대안들에 대한 비교 평가가 가능하다.

3.3 안전기능의 평가를 위한 시뮬레이션 모델 생성 및 평가 방법

3.1-3.2의 수행을 통해 모델링 결과를 활용한 안전 분석을 수행하게 된다. 이를 통해 위험원 식별 및 위험원 평가 까지가 수행이 된다. Activity Diagram을 활용한 빈도측면의 리스크 평가 결과에 기반하여 위험관리가 필요한 기능을 식별한다. 그 후 이 기능에 대한 안전 기능을 식별한다. 안전 기능은 기능의 고장 빈도를 줄여 리스크를 허용 가능 한 수준으로 낮추게 하는 기능이다. 고장을 모니터링 하는 기능, 동일 기능에 대한 redundancy, 기능의 확인 및 재수행 등 다양한 형태의 안전 기능을 정의 할 수 있다. 따라서 안전 기능을 어떤 형태로 결정하느냐에 따라 대상 시스템의 리스크 감소 정도가 결정된다. 본 논문에서는 Activity Diagram 상에 다양한 안전기능을 반영하여 각각에 대해 리스크를 시뮬레이션을 통해 평가하였다. 이를 통해 가장 고장 빈도를 줄일 수 있는 안전기능을 결정 할 수 있다. Fig. 6은 기능 수준에서의 설계대안의 개념과 평가방법에 대해 정의한 것이다. 거동모델에 고장을 표현하는 추가적인 거동을 반영한다. 그 후 안전기능이 식별되면 안전기능에 의한 추가적인 고장과 정상 상태사이의 분기를 반영한다. 이를 통해 일반 기능과 안전 기능들의 고장확률이 반영되면 전체 거동에서의 고장발생빈도를 평가 할 수 있다.

4. 철도신호시스템에 대한 설계대안 평가사례

4.1 SysML을 활용한 신호시스템 모델링

신호시스템의 안전 분석을 수행하기 위한 SysML모델링을 수행하였다. 모델링을 수행한 결과는 Fig. 7과 같다. Fig. 7과 같이 철도신호시스템의 기능, 물리적 구조에 대해 BDD를 통해 분석하였다. 기능적으로 열차의 제어와 운행정보를 관리하는 기능을 최상위 기능으로 한 하부 기능들을 도출하였다. 물리적으로는 지상, 차상, 정거장, 관제 부를 서브시스템으로 하여 물리적 구성에 대해 도출하였다. 식별한 기능들에 대하여 위험원 분석을 수행하게 된다.

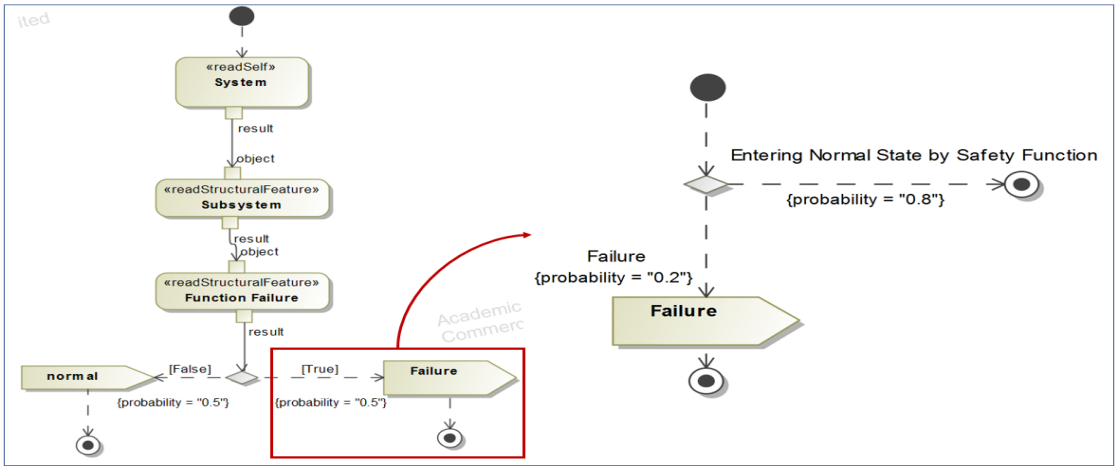

Fig. 6. Concept of Functional Level Design Alternative

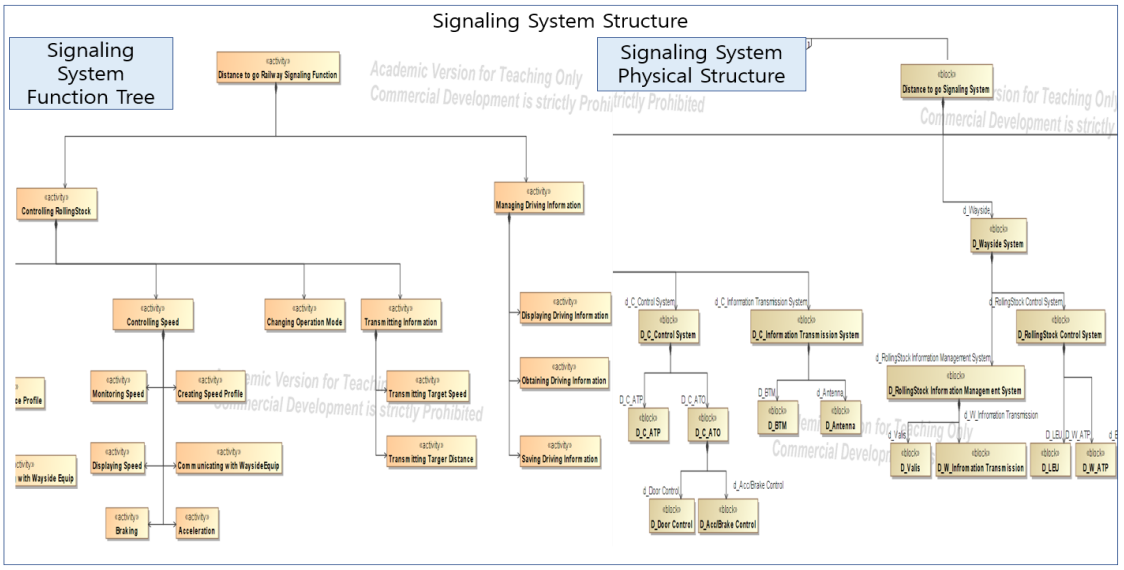

Fig. 7. Railway Signaling System Modeling Result: Structure

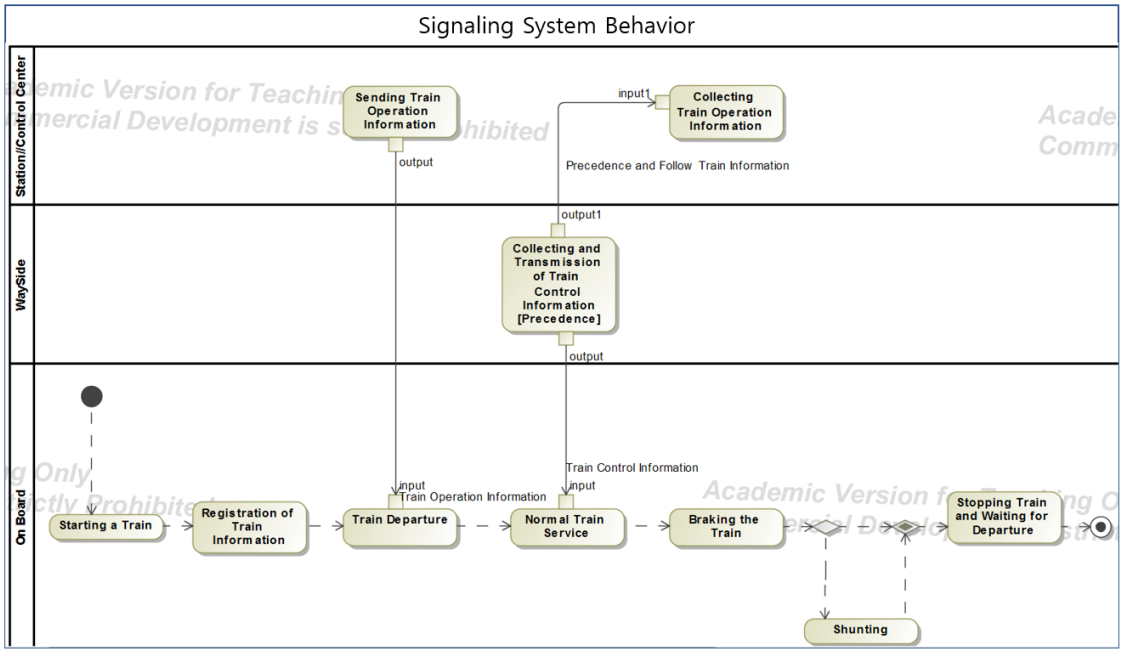

Fig. 8. Railway Signaling System Modeling Result: Behavior

4.2 신호시스템의 설계대안 평가

본 논문에서는 신호시스템에서 가장 핵심 기능 중에 하나인 데이터 전송기능에 대하여 열차의 출발 상황에서 위험원 분석을 수행하였다. Fig. 8과 같이 열차가 출발하는 상황에서 데이터 전송기능은 열차제어를 위한 핵심 기능 중 하나이다. 열차의 위치정보와 속도정보를 선, 후행 열차 및 관제부와 주고받으며 열차의 적정한 속도 및 열차 간 간격을 제어하는 데 중요한 역할을 한다. 데이터 전송과 관련된 위험원 들 중 본 논문에서는 잘못된 열차 제한속도 정보전송과 관련한 안전기능을 반영하였다. 잘

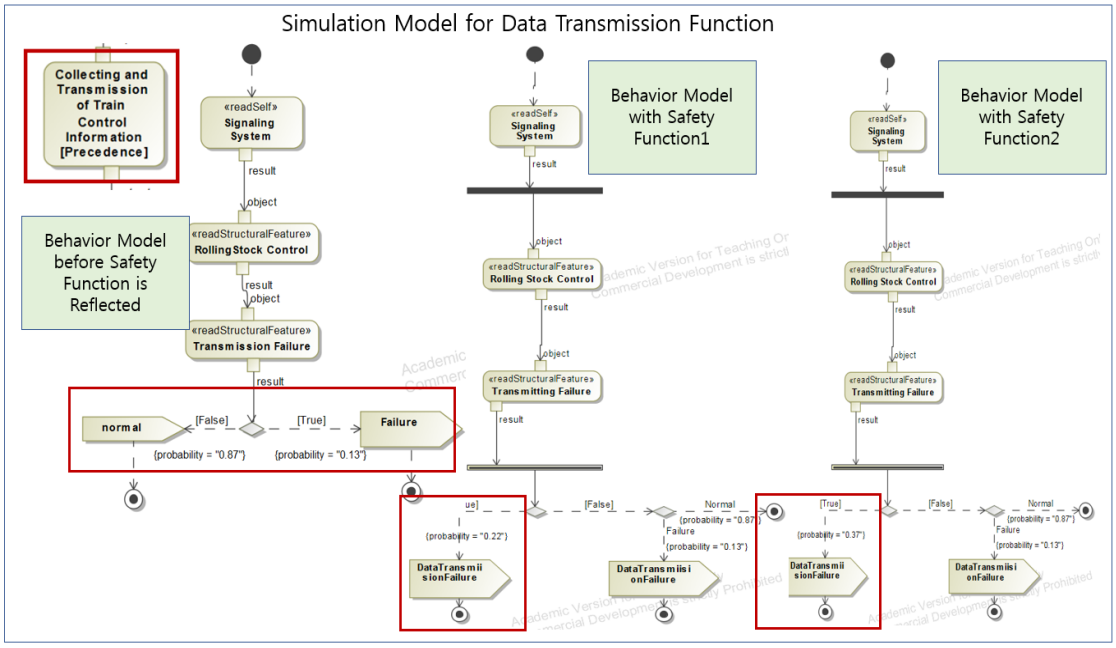

Fig. 9. Simulation Model for Data Transmission Function

못된 열차제한속도가 전송될 경우 열차의 속도가 제어에 오류가 발생하여 열차의 탈선 및 충돌을 유발할 수 있다. 현재 제한속도 전송오류의 확률은 0.13 정도로 평가 되었다. 이를 0.03 수준으로 빈도를 낮추기 위한 안전기능을 결정해야 하는데 이를 위한 시뮬레이션 모델을 Fig. 9와 같이 생성하였다. 좌측의 거동모델을 안전기능 반영 전의 모델로써 0.13의 전송오류 확률이 반영되어 있다. 중앙과 우측은 전송오류의 빈도를 줄이기 위한 안전기능이 반영되어 추가 분기가 반영된 모델이다. 안전기능1은 출발 전 입력되어 있던 제한속도 프로필의 값과 전송받은 제한속도 값을 비교하여 재전송하는 기능, 안전기능2는 동시에 두 개의 제한속도 값을 전송하는 기능을 도출하였다. 안전기능1의 경우 0.22의 오류 확률을 가지고 있고, 안전기능2의 경우 0.37의 오류 확률을 가지고 있다. 이것을 기존의 데이터 전송기능에 연결하였을 때 목표 고장빈도=기존의 고장빈도*안전기능의 고장빈도로 평가된다. 시뮬레이션에서는 반복적으로 거동이 수행되면서 목표 고장빈도를 지속적으로 평가하여 값을 도출하였다. 그 결과 안전기능1이 목표로 하는 0.03 이하인 0.028의 고장빈도로 평가 되었다. 이와 같이 안전기능이 식별되고 대상 기능과 안전기능의 고장 빈도가 결정되면 목표빈도를 충족하는 지 여부를 반복적인 시뮬레이션을 통해 확인 할 수 있다. 본 논문에서 제시한 방법을 통해 구성품수준에서 상세한 설계정보가 확보되기 전에 기능수준에서 안전기능의 형태로 안전 조치를 식별하여 비교평가를 수행하였다. 이를 설계에 반영하여 구현함으로써 안전 목표를 충족하는 설계를 수행 할 수 있다.

5. 결론

본 논문의 연구 목표는 기존에 구성품 수준에서의 안전 분석 및 안전조치의 결정이 이뤄지던 것을 기능수준에서 안전 분석 및 안전 목표를 충족하는 안전기능을 결정하기 위한 방법을 제시하는 것이다. 이를 위해 도출한 연구결과는 첫째, SysML을 활용한 대상 시스템의 모델링 방법을 제안하였다. 이를 통해 기능 수준에서 안전 분석에 필요한 설계정보들을 SysML모델을 통해 제공하였으며, 이를 활용하여 안전 분석을 수행하기 위한 SysML 모델과 안전 분석 활동 간의 연계성에 대해 제시하였다. 둘째, 기능수준에서 안전기능이 도출되었을 때, 안전 목표를 충족하는지 평가하기 위한 방법을 제안하였다. 이를 위해 SysML기반의 거동모델을 생성하고, 안전기능 반영전후의 고장 발생빈도를 시뮬레이션을 통해 평가하

는 방법을 제시하였다. 이를 통한 기대효과는 고장 발생 후의 피해를 경감시키는 것이 아닌 고장의 발생빈도 자체를 낮추기 위한 안전기능을 결정하는데 있어, 기능수준의 설계정보를 활용한 M&S를 통해 안전기능들이 안전 목표를 충족하는지를 평가 할 수 있다는 것이다.

References

[1] M. Bellotti, R. Mariani, "How future automotive functional safety requirements will impact microprocessors design", *Microelectronics Reliability*, Vol.50, No.9-11, pp.1320-1326, Sep. 30, 2010. DOI: https://doi.org/10.1016/j.microrel.2010.07.041

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

[3] A. F. Mehr, I. Y. Tumer, "Risk-based decision making for managing resources during the design of complex aerospace systems", *Journal of Mechanical Design*, Vol.128, No.4, pp.1014-1022, Jul. 30, 2006. DOI: https://doi.org/10.1115/1.2205868

[4] L. Li, B. Persaud, A. Shalaby, "Using micro-simulation to investigate the safety impacts of transit design alternatives at signalized intersections", *Accident Analysis and Prevention*, Vol.100, Mar. 30, 2017. DOI: https://doi.org/10.1016/j.aap.2016.12.019

[5] C. Hoyle, I. Y. Tumer, A. F. Mehr, W. Chen, "Health management allocation during conceptual system design", *Journal of Computing and Information Science Engineering*, Vol.9, No.2, pp.1-9, Jun. 30, 2009. DOI: https://doi.org/10.1115/1.3130775

[6] L. Tang, "Reliability assessments of railway signaling systems: A comparison and evaluation of approaches," Ph.D. dissertation, Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, Trondheim, Norway, Jun 2015

[7] Railway Applications - Communication Signalling and Processing Systems Software for Railway Control and Protection Systems, IEC Standard, IEC 62279, 2002.

[8] Road vehicles -- Functional safety, ISO Standard, ISO 26262, 2011.

[9] Functional safety - Safety instrumented systems for the process industry sector, IEC Standard, IEC 61511, 2016

[10] M. H. Ordouei, A. Elkamel, G. Al-Sharrah, "New simple indices for risk assessment and hazards reduction at the conceptual design stage of a chemical process", *Chemical Engineering Science*, Vol.119, No.8, pp.218-229, Nov. 2014. DOI: https://doi.org/10.1016/j.ces.2014.07.063

[11] T. Kurtoglu, I. Tumer, D. Jensen, "A functional failure reasoning methodology for evaluation of conceptual system architecture", *Research in Engineering Design*, Vol.21, No.4, pp.209-234, Oct. 2010. DOI: https://doi.org/10.1007/s00163-010-0086-1

[12] M. I. Campbell, "An evaluation scheme for assessing the worth of automatically generated design alternatives", *Research in Engineering Design*, Vol.20, No.1, pp.59-75, Mar. 30, 2009. DOI: https://doi.org/10.1007/s00163-008-0062-1

[13] System Modeling Language, Object Management Group Standard, 2015.

정 호 전(Ho-Jeon Jung) [정회원]

- 2010년 8월 : 경북대학교 전자공학과 (공학사)
- 2013년 2월 : 아주대학교 시스템공학과 (공학석사)
- 2013년 3월 ~ 현재 : 아주대학교 시스템공학과 (박사과정)

<관심분야>
시스템공학 (SE), 모델기반 시스템공학 (MBSE), 시스템 안전(System Safety), 기능안전(Functional Safety), 시스템 안전 관리체계, Modeling & Simulation 등.

이 재 천(Jae-Chon Lee) [정회원]

- 1977년 2월 : 서울대학교 공과 대학 전자공학과(공학사)
- 1979년 2월 / 1983년 8월: KAIST 통신시스템 (석/박사)
- 1984년 9월 ~ 1985년 9월 : 미국 MIT Post Doc 연구원
- 1985년 10월 ~ 1986년 10월 : 미국 Univ. of California 방문연구원
- 1990년 2월 ~ 1991년 2월 : 캐나다 Univ. of Victoria (Victoria, BC) 방문교수
- 2002년 3월 ~ 2003년 2월 : 미국 Stanford Univ. 방문교수
- 1994년 9월 ~ 현재 : 아주대학교 시스템공학과 정교수

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