Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 10 pp. 410-417, 2018

https://doi.org/10.5762/KAIS.2018.19.10.410
ISSN 1975-4701 / eISSN 2288-4688

시뮬레이션을 통해 안전성 검증을 위한 개선된 SysML 기반 고장 모델

김창원, 이재천*
아주대학교 시스템공학과

An Improved SysML-Based Failure Model for Safety Verification By Simulation

Chang-Won Kim, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 현대의 시스템은 지속적으로 대형화, 복잡화되어 왔기 때문에 시스템의 오류 발생 가능성이 커졌다. 시스템의 고장은 안전 사고를 발생시키고, 인명과 재산상의 막대한 피해를 줄 수 있다. 이러한 이유로 미 국방성과 IEC 등의 국제표준기구에서는 시스템의 안전성을 확보하기 위한 안전 관련 국제표준을 제정하였고, 시스템 설계와 안전 활동이 통합적으로 수행되어야 함을 권고하였다. 이에 따라 최근의 연구들은 모델기반 시스템 설계를 진행함과 동시에 모델을 활용하여 시스템의 안전성 검증을 수행하였다. 하지만 시스템 설계를 위한 모델과 안전성 분석 및 검증을 위한 고장모델을 서로 다른 모델링 언어를 기반으로 생성하였기 때문에 시스템 설계와 안전 활동이 통합적으로 수행되지 못하였다. 또한, UML 또는 SysML 기반으로 고장모델을 활용하여 안전 요구사항을 도출한 연구들은 안전 분석 및 검증에 고장모델이 제한적으로 활용되었다. 이와 같은 문제점을 해결하기 위해서 기존의 고장모델 활용법을 확장 시킬 필요가 있다. 우선 시스템 설계와 안전성 검증 활동을 통합적으로 수행할 수 있는 개선된 SysML 기반의 고장모델을 생성해야 한다. 다음으로 이 고장모델을 활용하여 도출된 안전 요구사항이 시스템 설계에 제대로 반영되었는지 검증할 수 있어야 한다. 따라서 본 논문에서는 개선된 SysML 기반 고장모델의 개념과 생성 절차를 제시하였고, 자동차 시스템에 대한 고장모델을 생성하였다. 또한, 자동차 시스템의 안전성을 검증하기 위해서 고장모델의 시뮬레이션을 수행하였다. 이를 통해서 개선된 SysML 기반 고장모델을 활용하여 시스템 설계와 안전성 검증 활동을 수행할 수 있음을 보였다.

Abstract System design errors are more likely to occur in modern systems because of their steadily increasing size and complexity. Failures due to system design errors can cause safety-related accidents in the system, resulting in extensive damage to people and property. Therefore, international standards organizations, such as the U.S. Department of Defense and the International Electrotechnical Commission, have established international safety standards to ensure system safety, and recommend that system design and safety activities should be integrated. Recently, the safety of a system has been verified by modeling through a model-based system design. On the other hand, system design and safety activities have not been integrated because the model for system design and the failure model for safety analysis and verification were developed using different modeling language platforms. Furthermore, studies using UML or SysML-based failure models for deriving safety requirements have shown that these models have limited applicability to safety analysis and verification. To solve this problem, it is essential to extend the existing methods for failure model implementation. First, an improved SysML-based failure model capable of integrating system design and safety verification activities should be produced. Next, this model should help verify whether the safety requirements derived via the failure model are reflected properly in the system design. Therefore, this paper presents the concept and method of developing a SysML-based failure model for an automotive system. In addition, the failure model was simulated to verify the safety of the automotive system. The results show that the improved SysML-based failure model can support the integration of system design and safety verification activities.

Keywords : Failure model, Integration model, Modeling and Simulation, SysML, SysML-based failure model, Safety verification

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 July 26, 2018 Revised September 21, 2018
Accepted October 5, 2018 Published October 31, 2018

1. 서 론

안전중시 시스템은 안전사고가 발생했을 때, 인명 손실과 재산상의 막대한 피해를 주는 시스템이다. 이 시스템의 안전성을 확보하기 위하여 안전관련 국제표준들이 제정되었다. 대표적인 안전관련 표준인 MIL-STD-882E, IEC 61508, ISO 26262등은 시스템 설계와 안전 활동의 통합을 권고한다[1-3]. 학계에서는 시스템 설계와 안전 활동을 통합하기 위해서 모델기반 접근법을 활용하였는데 그 이유는 첫째, 모델기반 시스템 설계는 시스템 설계의 일관성과 엔지니어들 사이의 의사소통을 향상 시킬 수 있다[4]. 두 번째, 모델의 시뮬레이션을 통해서 시스템의 성능과 제약사항 등을 검증하고, 시스템 최적화를 수행할 수 있다[5]. 이러한 이유로 시스템 설계와 안전 활동의 통합에 관한 초기 연구들은 메타 모델을 활용하여 시스템 엔지니어와 안전 엔지니어 사이의 의사소통 오류를 제거하고, 설계를 지원하였다[6, 7]. 하지만 메타 모델은 시스템 설계와 안전 활동의 통합 프로세스나 프레임워크를 제시하는데 국한되어서, 안전성 활동이 통합된 시스템 설계 방법론의 구체적인 제시가 미흡하였다.

이러한 이유로 최근에는 대상 시스템의 안전성 분석 결과들을 시스템 아키텍처에 반영한 고장모델 생성하였다. 이 고장모델을 활용하여 시스템의 안전 요구사항을 도출하고, 안전성을 검증하는 연구들이 수행되었다. 먼저, Model Based Safety Analysis (MBSA)는 고장모델을 생성하고, 이 고장모델을 안전성 검증에 적합한 모델로 변경하여 안전성 검증을 수행하였다[8-12]. 하지만 고장모델의 변환에 시간과 노력이 많이 소요된다. 이 문제를 해결하기 위해서는 하나의 모델링 언어를 통해서 시스템 설계와 안전성 검증을 수행할 수 있어야 한다. 다음으로 Mauborgne 등[13]과 Guiochet[14] 에서는 안전 요구사항을 도출하기 위해서 고장모델을 활용하는 데 중점을 두었다. 이러한 방법론을 안전성 분석이나 검증에 적용하기에는 어려움이 따른다.

위와 같은 문제점을 보완하고, 기존의 고장모델을 활용법을 확장시키기 위하여 본 논문에서는 개선된 SysML 기반 고장모델을 생성하고, 이를 활용하여 시스템 설계와 안전성 검증 활동을 수행하였다.

2. 선행연구 분석

2.1 안전성 검증을 위한 고장모델 활용에 관한 선행연구 분석

MBSA 연구들에서는 고장모델의 개념을 제시하였다. Joshi and Heimdahl[11]과 Papadopoulos 등[12]에서는 고장모델의 개념을 '시스템의 물리적 구성요소에서 발생 가능한 고장을 시스템 물리적 아키텍처 모델에 텍스트로 표현한 것'으로 설명하였다. Sharvia and Papadopoulos[8]에서는 '시스템의 설계 요소에 고장정보를 반영하여 설계 요소들의 잠재적인 고장과 그 영향을 나타낸 것'을 고장모델로 설명하였다. 결과적으로 고장모델은 '시스템의 기능 및 물리 아키텍처에 고장정보를 반영한 모델'이라 할 수 있다.

MBSA에서는 이러한 고장모델을 모델 체킹 도구의 언어를 사용하여 Formal specification으로 표현한다. 그 후, 고장모델에 대한 모델 체킹을 수행하여, 안전 요구사항에 위배되는 Counter-examples를 도출한다. 도출된 Counter-examples를 기반으로 고장모델을 수정함으로써 시스템의 안전 설계를 수행한다[15].

안전성 검증을 위해서 고장모델을 활용한 연구로 대상시스템에 대한 Failure Mode and Effect Analysis (FMEA)를 결과를 기반으로 고장모델을 생성하고, 모델 체킹을 수행하여 시스템 설계의 안전성을 검증한 방법론이 제시되었다[16]. 이 연구는 모델 체킹 도구의 언어인 SPIN 을 활용하여 안전 요구사항을 위배하는 모든 Counter-examples를 도출함으로써 발생 가능한 고장의 조합과 Accidents paths를 식별하였다. 하지만 위의 연구에서는 시스템 모델링과 모델 체킹을 통한 안전성 검증이 서로 다른 모델링 언어로 수행되었다. 이러한 방식은 모델의 변경에 시간과 노력이 소요된다. 따라서 하나의 모델링 언어를 사용하여 시스템 모델을 생성하고, 안전성 검증을 수행할 필요가 있다.

2.2 안전 요구사항 도출을 위한 고장모델 활용에 관한 선행연구 분석

고장모델은 안전성 검증뿐만 아니라 안전 요구사항을 도출하기 위해서 활용되었다. Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS) 방법론을 제시한 연구에서는 고장모델에 표현된 고장에 관한 정보를 기반으로 Fault Tree Analysis (FTA)를 수행하였다. 그리고 FTA 결과를 기반으로 FMEA를 수행하여 안전 요구사항을 도출하였다[8].

자동차 분야에서는 최상위 수준의 안전 요구사항인 안전 목표 (Safety goal)을 도출하기 위하여 SysML 기반 시나리오 모델을 활용하였다. 먼저 자동차 시스템의 위험원을 시스템의 정상 시나리오 모델에 반영하여 고장 시나리오 모델을 도출하였다. 다음으로 고장 시나리오 모델을 기반으로 안전 목표를 도출하고, 다시 고장 시나리오 모델에 반영하였다. 그 결과로 회피 시나리오 모델을 도출하였다[13]. UML을 활용하여 안전 요구사항을 도출한 연구에서는 UML의 Sequence diagram과 State machine diagram (STM)으로 시스템의 거동 모델을 표현하였다. 시스템 거동 모델과 가이드 워드를 활용하여 Hazard & Operability Study (HAZOP)를 수행함으로써 안전 요구사항을 도출하였다[14].

위의 방법론은 고장모델을 활용하여 안전 요구사항을 도출하는 데 중점을 두어서 안전성 분석이나 검증에 적용하기에 한계가 있다.

2.3 문제정의 및 연구목표

기존의 고장모델은 안전 분석, 안전 요구사항 도출 및 검증을 위하여 활용되었다. 먼저, 안전성 분석 및 검증을 수행하기 위하여 고장모델을 활용한 연구들은 모델 체킹을 수행하기 적합하도록 고장모델을 변경하는 데 시간과 노력이 소요되었다. 이를 해결하기 위하여 고장모델을 변경하지 않고, 안전성 검증을 수행할 수 있어야 한다. 다음으로 고장모델을 기반으로 안전 요구사항을 도출하기 위한 연구들은 안전 요구사항을 도출하기 위하여 고장모델을 변경할 필요는 없었다. 하지만 요구사항을 도출하는데 국한되었다. 따라서 기존의 고장모델의 활용법을 확장시킬 필요가 있다. 이에 본 연구에서는 개선된 SysML 기반 고장모델을 생성하였고, 이 모델의 시뮬레이션을 수행하여 시스템의 안전 설계를 검증하였다.

이어지는 3절에서는 기존의 고장모델을 개선한 SysML 기반 고장모델을 생성하였다. 4절에서는 SysML 기반 고장모델의 시뮬레이션을 통해서 안전 설계를 검증하였다.

3. 개선된 SysML 기반 고장모델의 생성 방법

고장은 시스템의 구성요소에 할당된 기능이 설계 의도대로 작동하지 않는 것을 의미한다. 시스템의 기능 아키텍처에 기능 오작동을 반영함으로써 고장을 시스템 아키텍처 모델에 반영할 수 있다. SysML은 시스템의 기능 및 물리 아키텍처를 모델링하기 위한 언어이기 때문에 고장정보를 시스템 모델의 요소로서 시스템 아키텍처에 반영하기 적합한 모델링 언어이다. 따라서 본 논문에서는 SysML을 활용하여 시스템 모델에 고장정보를 반영한 고장모델을 생성하였다.

3.1 SysML 기반 시스템 아키텍처 모델 생성 방법

SysML 기반 고장모델을 생성하기 위해서 먼저, 고장정보를 반영할 수 있는 시스템 아키텍처를 설계해야 한다. 다음으로 시스템 아키텍처의 정보를 활용하여 Functional FMEA를 수행함으로써 시스템의 고장정보를 도출한다. 위의 활동으로 도출된 시스템의 고장정보를 SysML 요소로 표현하기 위해서 고장정보와 SysML의 모델요소를 맵핑한다. 마지막으로 시스템 아키텍처에 Functional FMEA 결과를 반영한 고장모델을 생성한다. Fig. 1에 SysML 기반 고장모델을 생성하기 위한 절차를 정리하였다.

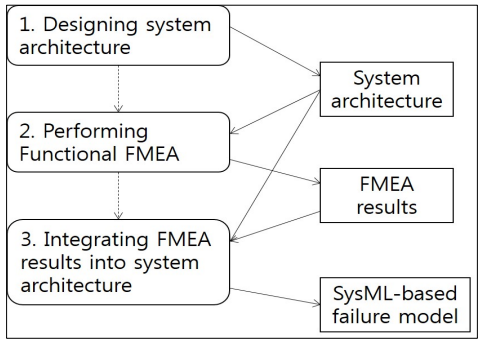

Fig. 1. General procedure for SysML-based failure model development.

Fig. 1의 첫 단계로 고장정보가 반영되지 않은 정상 상태의 시스템 아키텍처를 생성해야 한다. 시스템 설계 초기에는 상세한 시스템의 물리 구조가 도출되지 않기 때문에 시스템 기능 아키텍처를 생성하여 거동을 분석하여야 한다. 먼저, Activity diagram (ACT)는 시스템의 기능과 기능 사이의 데이터 교환 및 순서 관계를 표현할 수 있어서 시스템 거동을 분석하기에 적합한 다이어그램

이다. Fig. 2는 일반적인 시스템의 기능 아키텍처를 ACT로 나타낸 것이다.

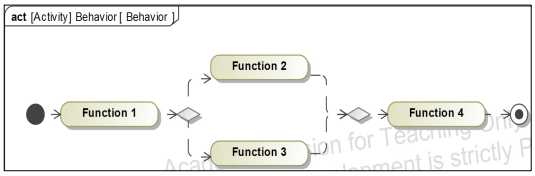

Fig. 2. Activity diagram: general system behavior model.

Fig. 2의 기능 아키텍처는 고장에 대한 안전 요구사항이 반영되지 않은 기능 아키텍처이다. 즉, 시스템이 정상 상태에서 어떻게 거동하는지 분석할 수 있다. 이 기능 아키텍처를 기반으로 시스템 설계 초기의 고장정보를 도출하기 위하여 Functional FMEA를 수행하는 것이 고장모델 생성의 두 번째 단계이다. Functional FMEA는 시스템의 기능에 대한 고장모드를 분석하고, 그 영향을 평가하는 활동이다. 이 활동을 통해서 시스템 기능의 고장모드, 그 고장이 시스템에 미치는 영향 및 안전 요구사항 등이 도출된다. 안전 요구사항을 통해서 안전 조치가 도출되고, 이러한 고장정보를 시스템 모델에 통합시킴으로써 SysML 기반 고장모델을 생성할 수 있다. 또한, Functional FMEA 결과로 도출된 안전 조치를 기능 아키텍처에 반영하고, 이 기능 아키텍처에 대한 시뮬레이션을 수행하면, 안전 조치가 제대로 동작하는지 검증할 수 있다.

3.2 고장정보를 반영한 개선된 SysML 기반 고장모델 생성 방법

Functional FMEA의 산출물은 워크시트의 형태로 존재하기 때문에 이것을 시스템 모델에 바로 반영하기 어렵다. 이 문제점을 해결하기 위해서 Functional FMEA 결과를 STM의 모델요소와 맵핑시킬 필요가 있다. 시스템 모델은 안전 분석을 수행하기 전의 모델로서 시스템의 정상 상태에 대한 모델이다. 고장모델은 이러한 시스템의 정상 상태 모델에 고장정보를 추가하여 비정상적인 상태의 거동을 나타내야 한다. STM은 시스템의 상태를 나타내고, 각 상태에서의 거동 및 시스템의 상태가 전이되는 것을 표현할 수 있다. 즉, STM은 시스템이 정상 상태, 비정상 상태 (고장이 발생했으나 시스템 전체에 영향을 미치지 않는 상태)와 고장 상태를 표현하고, 각 상태에서의 거동을 표현할 수 있다. 또한, 정상 상태에서 비정상 상태로 (반대의 경우도 성립), 다시 비정상 상태에서 고장 상태로 전이되는 것을 표현하기 적합하다. Table 1은 Functional FMEA 수행 결과로 도출된 고장정보들과 STM의 모델 요소를 맵핑한 것이다.

Table 1. Mapping Functional FMEA to state machine diagram elements.

Functional FMEA elements	State machine diagram elements
Function	Action node of Do activity
Failure mode	Transition path
Immediate effect	State
System effect	State

SysML 기반 고장모델 생성의 마지막 단계는 고장정보를 시스템 모델에 통합하는 것이다. Table 1을 기반으로 시스템의 정상 상태, 비정상 상태 및 비정상 상태에서 안전 조치가 작동하지 않았을 때의 상태를 State node로 나타내었다. 또한, 시스템의 기능과 안전 조치 (Recommended actions)을 Do activity의 action node로 표현함으로써 각 상태 (정상, 비정상, 고장 상태)에서 시스템이 어떻게 거동하는지 표현하였다. 마지막으로 고장의 발생하였을 때, 안전 조치가 작동하는 경우와 작동하지 않는 경우를 transition path로 표현하였다. 위의 단계들을 수행함으로써 Fig. 3과 같은 SysML 기반 고장모델이 생성하였다.

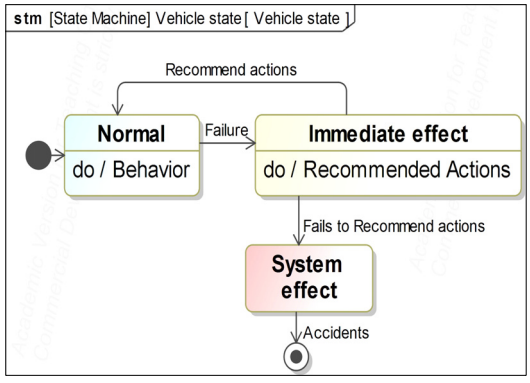

Fig. 3. Generalized SysML-based failure model.

Table 2. Functional FMEA results of automotive braking system.

Functional Failure Mode and Effects Analysis				
Function	Failure mode	Immediate effect	System effect	Recommended actions
Control caliper	Ineffective control	Unable to control caliper	Unable to decelerate automobile	1. Diagnose the cause of failure 2. Incorporate an auxiliary caliper regulatory function

4. 자동차 시스템의 안전성 검증을 위한 SysML 기반 고장모델의 활용

본 논문에서는 SysML 기반 고장모델을 생성하는 것 뿐만 아니라 생성된 SysML 기반 고장모델 안전성 검증에 활용하는 것이 목적이다. 안전성 검증에 SysML 기반 고장모델을 활용할 수 있음을 보이기 위해서 자동차 제동 시스템을 대상으로 고장모델을 생성하였고, 시뮬레이션을 통해서 시스템의 안전 설계를 검증하였다.

4.1 자동차 제동 시스템에 대한 SysML 기반 고장모델 생성

자동차 제동 시스템에 대한 고장모델을 생성하기 위해서 우선, 대상시스템에 대한 아키텍처를 생성해야 한다. 그 후, 생성된 시스템 아키텍처를 기반으로 Functional FMEA를 수행하여 제동 시스템에 대한 고장정보를 도출하여야 한다. 본 논문에서는 자동차 바퀴에 제동력을 가하는 '캘리퍼 컨트롤 기능'에 대한 Functional FMEA를 수행하였다. Table 2는 '캘리퍼 컨트롤 기능'에 대한 Functional FMEA 수행 결과를 정리한 것이다.

Functional FMEA 결과 '캘리퍼 컨트롤 기능'의 고장이 발생하면, 비정상 상태인 '캘리퍼 컨트롤 기능 불가' 상태가 된다. 이 상태에서 안전 조치가 작동되면 다시 정상적으로 제동이 수행된다. 하지만 '캘리퍼 컨트롤 기능 불가' 상태가 지속되면, 고장 상태인 '자동차 감속 기능 불가' 상태가 된다. 이러한 비정상 상태를 제어하기 위하여 안전 조치로서 '캘리퍼 컨트롤 기능'을 진단할 수 있는 기능과 고장에 대비한 기능인 '진단 기능'과 '캘리퍼 컨트롤 예비 기능'을 도출하였다.

Table 2의 결과를 시스템 아키텍처에 통합하기 위해서는 Table 1을 활용하여야 한다. Table 1을 기반으로 고장정보를 시스템 아키텍처 모델에 반영하였다. Fig. 4는 자동차 제동 시스템에 대한 고장모델을 생성한 것이다.

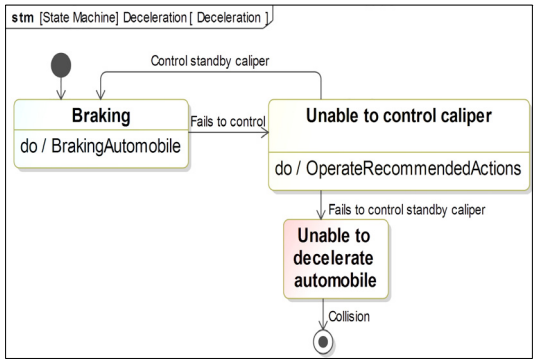

Fig. 4. SysML-based failure model of an automotive braking system.

Fig. 4의 고장모델은 정상적인 제동상태와 '캘리퍼 컨트롤 기능 불가' 및 안전 조치가 작동하지 않았을 때의 '자동차 감속 기능 불가' 상태를 보여준다. 또한, 각 상태에서 수행되는 거동을 Do activity로 표현함으로써 시스템이 정상 상태와 비정상 상태일 때, 어떤 거동을 수행하는지 확인할 수 있다. 마지막으로 각 상태는 고장 발생 여부와 과 안전 조치의 작동 여부에 의하여 전이되는 것을 확인할 수 있다.

4.2 SysML 기반 고장모델을 활용한 안전 조치의 검증

Fig. 4의 고장모델은 자동차 시스템이 제동에 관한 거동을 수행할 때, 발생할 수 있는 고장에 대한 안전 조치를 시스템 아키텍처에 반영한 모델이다. Fig. 5는 제동 시스템의 거동과 안전 조치가 반영된 기능 아키텍처를 ACT로 생성한 것이다. 먼저, 각 기능이 할당된 시스템의 물리 요소들이 스윔레인 (Swim-lanes)에 표현되었다. 다음으로 테두리가 둥근 회색 직사각형 (F.1 ~ F.4)는 정상 상태에서 수행되는 제동에 관한 기능들이다. 마지막으로 테두리가 둥근 청록색 직사각형 (S.F.1 ~ S.F.2)는 '캘리퍼 컨트롤 기능'의 고장에 대한 안전 조치이다. 즉, '캘리퍼 컨트롤 기능'의 고장에도 제동 시스템이 안전한

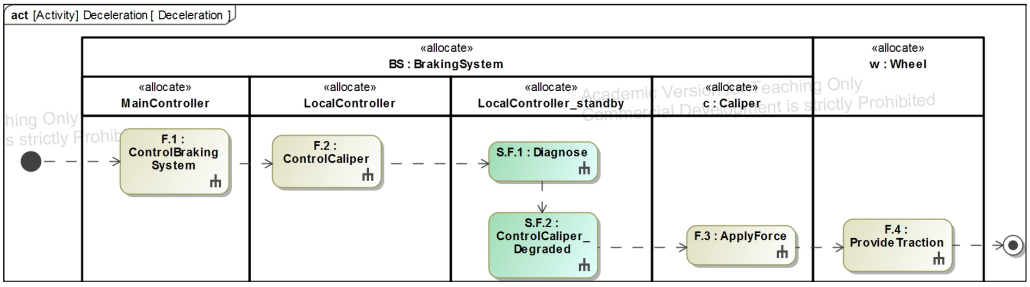

Fig. 5. Behavioral model of automotive braking system with safety measures.

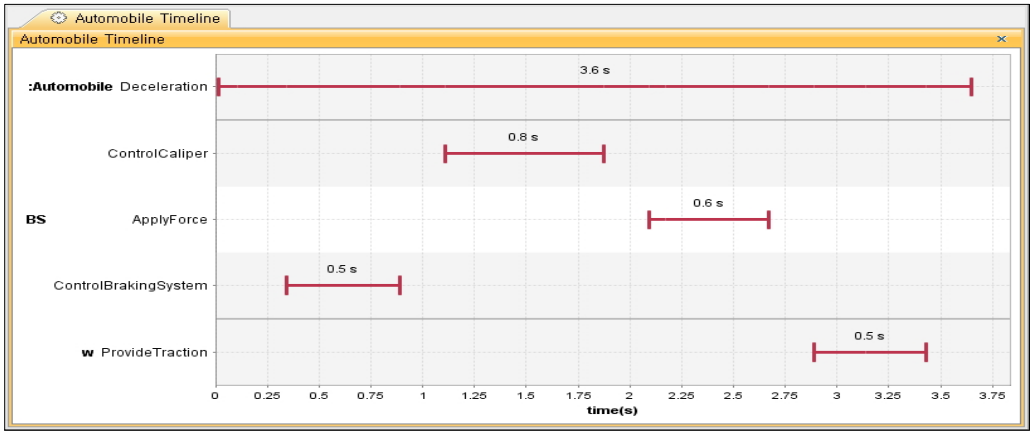

Fig. 6. Simulation of the behavior of the automotive braking system without safety measures.

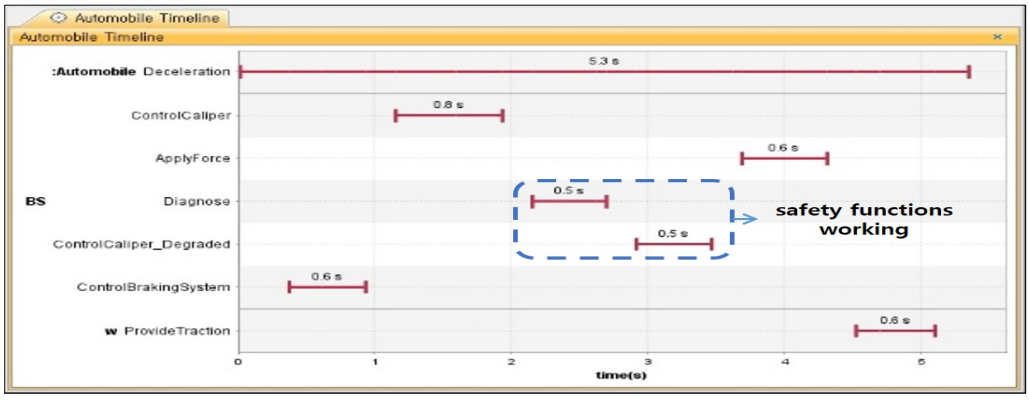

Fig. 7. Simulation of the behavior of the automotive braking system with safety measures.

상태를 유지할 수 있도록 시스템 아키텍처를 수정하였다.

시스템 기능 아키텍처에 안전 조치가 제대로 반영되었는지 검증하기 위해서 거동 시뮬레이션을 수행하였다. 먼저, 정상적인 상태에서 제동에 대한 기능 아키텍처를 시뮬레이션하였고, 그 결과를 Fig. 6에 나타내었다. 제동을 수행할 때, '브레이킹 시스템 컨트롤 기능', '캘리퍼 컨트롤 기능', '포스 적용 기능', '트랙션 제공 기능' 순으로 제동에 관한 기능들이 수행되는 것을 확인할 수 있다. 다음으로 안전 조치가 반영된 제동의 기능 아키텍처를 시뮬레이션하였고, 그 결과를 Fig. 7에 나타내었다.

‘캘리퍼 컨트롤 기능’의 고장이 발생하였고, 이에 대응하는 안전 조치가 작동한 것을 확인할 수 있다. 결과적으로 ‘브레이킹 시스템 컨트롤 기능’이 동작하고, ‘캘리퍼 컨트롤 기능’의 고장을 ‘진단 기능’이 감지하여, ‘캘리퍼 컨트롤 예비 기능’이 수행된 것을 확인할 수 있다. 이후에 ‘포스 적용 기능’, ‘트랙션 제공 기능’이 순차적으로 수행되는 것을 확인할 수 있다.

Fig. 7의 시뮬레이션 결과는 자동차 제동 시스템에 대한 고장모델을 활용하여 안전 조치가 시스템 아키텍처에 제대로 반영되었는지에 대한 안전 설계를 검증할 수 있음을 보였다.

5. 결론

본 연구에서는 시스템 아키텍처에 고장정보를 반영한 SysML 기반 고장모델을 생성하였다. 다음으로 안전 조치를 SysML 기반 고장모델에 반영하였다. 이 모델의 시뮬레이션을 수행하여 시스템 아키텍처에 대한 안전 설계가 제대로 수행되었는지 검증하였다.

본 연구에서 제시한 SysML 기반 고장모델 생성 방법론은 SysML로 시스템 모델을 생성하고, 여기에 고장정보를 반영함으로써, 시스템 모델을 모델 체킹을 위한 고장모델로 변경할 필요가 없다. 따라서 기존의 고장모델을 활용한 안전성 검증 방법보다 시간과 노력이 적게 소요된다. 또한, 안전 요구사항 도출을 위해서 고장모델을 활용한 것에 국한되었던 기존의 고장모델의 활용법을 확장 시켰다. 추후의 연구는 SysML 기반 고장모델을 활용하여 안전 분석까지 수행함으로써 본 연구 결과를 향상시킬 필요가 있다.

References

[1] Department of Defense Practice: System Safety, Department of Defense Standard, MIL-STD-882E, 2012.

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

[3] Road Vehicles - Functional Safety, ISO Standard, 26262, 2011.

[4] C. Paredis, "Model-Based Systems Engineering: A roadmap for academic research", in Lecture, Atlanta, Georgia, 2008.

[5] S. Friedenthal, "Model Based Systems Engineering NASA PM Challenge 2009", in Lecture, Feb. 25, 2009.

[6] P. Y. Piriou, J. M. Faure, and G. Deleuze, "A meta-model to support the integration of dependability concerns into systems engineering processes: An example from power production", *IEEE Systems Journal*, Vol.10, No.1, pp. 1-10, Jul. 9, 2014.
DOI: https://doi.org/10.1109/jsyst.2014.2328663

[7] M. Hillenbrand, M. Heinz, J. Matheis, and K. D. Müller-Glaser, "Development of Electric/Electronic Architectures for Safety-Related Vehicle Functions", *Software: Practice and Experience*, Vol.42, No.7 pp. 817-851, Jan. 31, 2012.
DOI: https://doi.org/10.1002/spe.1154

[8] S. Sharvia and Y. Papadopoulos, "Integrating Model Checking with HiP-HOPS in Model-Based Safety Analysis", *Reliability Engineering and System Safety*, Vol.135, pp. 64-80, Mar. 2015.
DOI: https://doi.org/10.1016/j.ress.2014.10.025

[9] G. Duan, J. Tian, and J. Wu, "Extended FRAM by integrating with model checking to effectively explore hazard evolution", *Mathematical Problems in Engineering*, Vol.2015, Oct. 31, 2015.
DOI: https://doi.org/10.1155/2015/196107

[10] H. Mehrpouyan, "Model-Based hazard analysis of undesirable environmental and components interaction", M.S. thesis, Department of Computer and Information Science, Linköping University, Linköping, Sweden, Aug. 2011.

[11] A. Joshi and M. P. E. Heimdahl, "Behavioral fault modeling for model-based safety analysis", in Proc. High Assurance Systems Engineering Symposium, Plano, TX, Nov. 14, 2007, pp. 199-208.

[12] Y. Papadopoulos, J. McDermid, R. Sasse, and G. Heiner, "Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure", *Reliability Engineering & System Safety*, Vol.71, No.3, pp. 229-247, Mar. 31, 2001.
DOI: https://doi.org/10.1016/s0951-8320(00)00076-4

[13] P. Mauborgne, S. Deniaud, E. Levrat, E. Bonjour, J.-P. Micaëlli, and D. Loise, "Operational and System Hazard Analysis in a Safe Systems Requirement Engineering Process – Application to automotive industry", *Safety Science*, Vol.87, pp. 256-268, Aug. 2016.
DOI: https://doi.org/10.1016/j.ssci.2016.04.011

[14] J. Guiochet, "Hazard analysis of human‐robot interactions with HAZOP‐UML", *Safety Science*, Vol.84, pp. 225-237, Apr. 30, 2016.
DOI: https://doi.org/10.1016/j.ssci.2015.12.017

[15] O. Jaradat, "Automated architecture-based verification of safety-critical systems", M.S. thesis, School of Innovation, Design and Engineering, Malardalen University, Vasteras, Sweden, Feb. 2012.

[16] Q. Wei, J. Jiao, and T. Zhao, "Flight control system failure modeling and verification based on SPIN", *Engineering Failure Analysis*, Vol.82, Apr. 18, 2017.
DOI: https://doi.org/10.1016/j.engfailanal.2017.04.004

김 창 원(Chang-Won Kim) [정회원]

- 2014년 2월 : 한밭대학교 산업경영공학과 (공학사)
- 2014년 3월 ~ 현재 : 아주대학교 시스템공학과 (석·박사통합과정)

<관심분야>
시스템공학 (SE), Model-based SE (MBSE), System Safety, Functional Safety, Modeling & Simulation

이 재 천(Jae-Chon Lee) [정회원]

- 1977년 2월 : 서울대학교 공과 대학 전자공학과(공학사)
- 1979년 2월 : KAIST 통신시스템 석사
- 1983년 8월 : KAIST 통신시스템 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